VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Implementace steganografie v IP sítích

Steganography Implementation in IP networks

2018 **Bc. Ivo Kostecký**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání diplomové práce

Student: **Bc. Ivo Kostecký**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: Implementace steganografie v IP sítích
Steganography Implementation in IP networks

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem práce je vývoj řešení, demonstrujícího možnosti tvorby skrytého kanálu pro přenos informací v hlavičkách běžně používaných protokolů protokolové rodiny TCP/IP.

1. Prostudujte princip steganografie, její existující aplikace, a popište je.
2. Vyberte protokoly na 3.-7. vrstvě ISO-OSI modelu vhodné pro přenos utajených informací a určete, které části hlaviček je k přenosu možno využít.
3. Navrhněte a implementujte skrytý kanál, využívající hlaviček alespoň 3 vybraných protokolů (vyjma UDP), výsledné řešení implementujte a otestujte.
4. Zhodnoťte, zda použití konkrétní varianty steganografie ovlivnilo vytvořená spojení (např. zda nebyly pakety během přenosu zahozeny).
5. Proveďte odhad dosažitelné bitové rychlosti skrytého kanálu, otestujte skutečné množství přenesených dat v podmínkách pevné, bezdrátové a buňkové sítě a výsledky vyhodnoťte.

Seznam doporučené odborné literatury:

1. Murdoch S.J., Lewis S.: Embedding Covert Channels into TCP/IP. [online] [cit 2016-02-11]. Dostupné z URL: <http://sec.cs.ucl.ac.uk/users/smurdoch/papers/ih05coverttcp.pdf>

2.Dhobale, D., Ghorpade, V.R., Patil B.S., Patil S.B.: Steganography by hiding data in TCP/IP headers. 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). [online] [cit 2016-02-11]. Dostupné z URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5579643>.

3. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker: Digital Watermarking and Steganography, 2nd Edition. Elsevier / Morgan Kaufmann, 2007, 624 stran, ISBN: 978-0-08-055580-5.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Pavel Moravec, Ph.D.**

Datum zadání: 01.09.2016

Datum odevzdání: 30.04.2018

doc. Ing. Jan Platoš, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: 24. dubna 2018

Bc. Ivo Kostecký

Abstrakt

Steganografie popisuje způsob přenosu informace způsobem, který není viditelný pro neseznámené pozorovatele. Tato práce se zabývá smyslem použití skrytého komunikačního kanálu v prostředí počítačových sítí, zmiňuje jeho historickou roli a dodává jeho současný účel.

V teoretické části je dekomponován návrh steganografického kanálu. Nejprve je proveden rozbor vhodných protokolů, a dále části jejich hlaviček vhodných k tomuto účelu. V práci byl kladen důraz na používání konstrukčních prvků a postupů známých z jiných síťových protokolů.

Demonstrační program vytvořený v praktické části využívá záhlaví protokolů IP, ICMP, DNS a HTTP pro přenos steganografických informací. Je provedeno měření vytvořeného skrytého kanálu s důrazem na zjištění přenosové kapacity, interference s ostatním síťovým provozem a zařízeními. Výsledky jsou zasazeny do kontextu scénářů potencionálního nasazení či obrany proti použití.

Klíčová slova

steganografie, skrytý kanál, IP sítě, steganografický framework, kybernetická bezpečnost

Abstract

Steganography describes the way of information transfer to such a degree that is invisible for an unaware viewer. This work describes the meaning of usage in computer network covered channel. Furthermore, it is mentioning its role in history and adding today's meaning.

Theoretical part decomposes the design of steganography channel. First the suitable protocols are selected alongside with their headers that can be used for the purpose of transferring data. During the research the emphasis was on the usage of construction parts and methods which are well known from other network protocols.

The demonstrational program works as the practical part output and it is using the headers of protocols IP, ICMP, DNS and HTTP for transferring steganographical information. Later the created covered channel is being measured with the emphasis on the determination of transmission speed and interference with other traffic or network devices. The results can be used in the context of deployment's usage cases or defensive approaches.

Key words

steganography, covered channel, IP networks, steganography framework, cyber security

Obsah

Seznam použitých zkratek a symbolů

Zkratka	Význam
API	Application Programming Interface
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
b	bity
C#	objektově orientovaný programovací jazyk platformy .NET Framework
CERT/CSIRT	Computer Emergency Response Team / Computer Security Incident Response Team
CRC	Cyclic Redundancy Check
DMZ	Demilitarized Zone
DNS	Domain Name Systém
hotspot	bezdrátový přípojný bod k internetu
HTTP	Hypertext Transfer Protocol
CHAP	Challenge Handshake Authentication Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Systém
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention Systém
ISO/OSI	International Organization for Standardization / Open Systems Interconnection model
LAN	Local Area Network
loopback	rozhraní zpětné smyčky
MAC	Media Access Control
MD5	Message-Digest Algorithm 5
ms	Milisekundy
NAT	Network Address Translation
OS	Operační systém
PAP	Password authentication protocol
QoS	Quality of Service
RFC	Request For Comments, sada doporučení
s	sekundy
TCP	Transmission Control Protocol
TCP/IP	sada protokolů pro komunikaci v počítačové síti
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VŠB-TUO	Vysoká škola Báňská – Technická univerzita Ostrava

Seznam ilustrací

Seznam tabulek

Úvod

Již po staletí jsou základem mnoha odvětví lidských činností informace a práce s nimi. Od prvopočátků se taktéž řeší způsoby, jakými klíčové informace ochránit před zneužitím či únikem. Všeobecný vývoj přináší nové technologie od fyzických po elektronické, které přispívají jednak k možnosti s daty pracovat v doposud nepředstavitelném měřítku, na druhou stranu také rozšiřuje místa i způsoby, jakými mohou informace uniknout do nežádoucích rukou.

Obor informačních technologií je těsně spojen se způsoby nakládání s informacemi, jak už z jeho názvu vyplývá, nicméně jeho úkolem je taktéž umět je ochránit. Na rozdíl od řešení bezpečnostních otázek před nástupem elektronických médií si musí současný obránce poradit s faktem, že většinu z bezpečnostních hrozeb nejde vidět pouhým zrakem a je potřeba uvažovat o každé vrstvě, kterou informace prostupuje, jako o místě potenciálního ohrožení.

Tato práce se zabývá jednou ze zmíněných vrstev, a tou je síťová konektivita a v ní hledání prostoru pro steganografii. Důvodem, proč se zabývat bezpečností na této úrovni je fakt, že je všudypřítomná a svým způsobem tak samozřejmá, že málokdo by v ní hledal tento druh nebezpečí.

Pro větší názornost se nabízí paralela z běžného života – pokud policie hledá u silnice v projíždějících vozech zakázaný náklad, pak s největší pravděpodobností bude nahlížet do zavazadlových prostor či na sedadla, a pokud nebude mít důvodné podezření, nepodrobí zvláštní prohlídce vozidlo jako takové. S jistou nadsázkou lze tedy říct, že tato práce se zabývá způsoby, jak kombinací barvy, typu a dalších specifických vlastností vozidla doručit informaci tak, aby si tohoto přenosu policie nevšimla.

Ačkoliv použité technologie a přístupy připomínají spíše útočníkovy nástroje, úkolem výzkumu v této oblasti je dozvědět se, jakých technik přenosu je možné zneužít nebo objevit slabosti současných systémů a použít proti nim odpovídající obranné a preventivní postupy. Tohoto se nejlépe dosahuje etickým hackingem, jehož představitelem jsou práce tohoto typu.

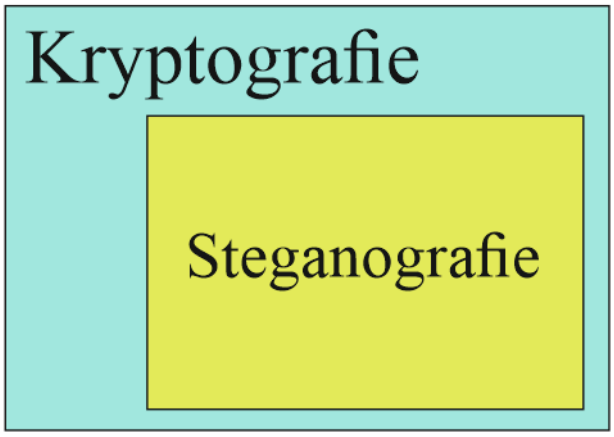
Výstupem praktické části práce je počítačový program, který ověřuje teoretické teze ukrývání zpráv v hlavičkách dnes nejčastěji nasazené rodiny protokolů. Rovněž umožňuje testování průchodu datového provozu v existujících obranných mechanismech. Na následujících stránkách se uvádějí nezbytné teoretické informace k pochopení problematiky a dále úvahy, které vedly ke konstrukci výsledných řešení.

1 Princip steganografie a existující aplikace

1.1 Princip steganografie

Technika steganografie je způsobem ukrytí zprávy před nežádoucími osobami či subjekty do jiné regulérní zprávy během jejího předávání v různých prostředích. V ideálním případě ji mohou získat pouze ti příjemci, kteří jsou s její existencí a detaily ukrytí předem seznámeni. Nezúčastněný pozorovatel by se měl domnívat, že tato zpráva je běžnou a její obsah standardním, pakliže vůbec o přenosu ví. Pokud se podaří takový způsob výměny komunikace realizovat, je nazýván skrytým kanálem.

Je důležité už v úvodu poznamenat, že tato metoda se vzájemně doplňuje s kryptografií, resp. je její podmnožinou, nicméně v každé platí jiný bezpečnostní princip. **Kryptografie** znemožňuje zprávy přečíst bez jejich rozluštění a zjistit tak jejich obsah, nicméně existence takové komunikace je v okolí zřejmá. **Steganografie** se snaží nevzbudit ani podezření, že jsou nějaké informace vyměňovány, ale v případě odhalení můžou být prostředníky přečteny. Logicky se tedy nabízí jejich kombinace pro dosažení vyššího utajení.



Obrázek 1.1: *Disciplína steganografie je podoborem disciplíny kryptografie*

Klíčový princip pěkně demonstruje následující příklad. Nechť páry Alice a Bob, Carol a Dave společně hrají **karetní hru Bridge**. Tato hra je určena pro dvě dvojice hráčů, které jsou rozsazeny kolem stolu tak, že spoluhráči sedí proti sobě a jejich soupeři křížem [2]. Principem úspěšné hry je se tajně ve dvojici shodnout na výši obdržených karet, což Alice s Bobem provádí pomocí nenápadných posunků, jejichž význam je znám pouze jim. V záplavě dalších běžných pohybů jsou tak tato gesta steganograficky ukryta před zraky soupeřícího páru. Kdyby Carol s Davem chtěli namísto steganografických posunků použít kryptografii pro vyrozumění se o svých kartách, mohli by na sebe promluvit nějakým cizím jazykem, o kterém si budou jisti, že mu Alice s Bobem nerozumí. Nicméně pak by bylo Alici s Bobem jasné, že tito dva hráči se již dohodli, a pro další kolo by mohli zavést například pravidlo o zákazu mluvení během hry.

Obrázek 1.2: *Uspořádání hráčů při hře bridge [1]*

Analogie se hrou bridge je ostatně pro vysvětlení pozadí steganografie velmi výhodná. Při této hře je zřejmé, že se partneři mezi sebou budou domlouvat, ale protihráčům není jasné jak. Mohou se snažit jejich vzájemné interakce zachytit a pokusit se v nich zprávy o obdržených kartách rozpoznat. Kvalita či komplikovanost zvolené techniky pak rozhodnou o vítězství či prohře spoluhráčů.

1.2 Základní pojmy

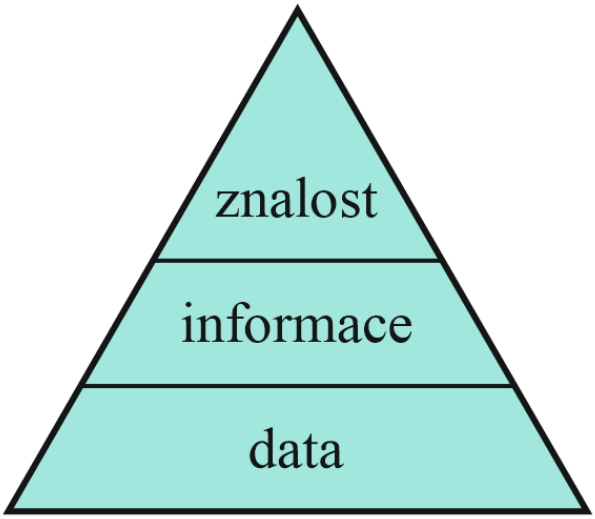
Jako v každé jiné specializované oblasti používá obor steganografie své specifické pojmy, které mohou snadno splývat, je proto žádoucí provést základní orientaci. Samotné slovo steganografie pochází z řečtiny – stegos = skrytý, graphein = psát [3].

Steganografie při svém nasazení vytváří **skrytý kanál** (covert channel), který je určen k přenosu utajené informace. Na rozdíl od šifrovaného kanálu, kdy je přenos vidět, ale není mu rozumět, je skrytý kanál opakem – bylo by mu rozumět, ovšem kdyby byl vidět.

Jako médium přenosu, tzv. **nosič,** používáme v síťovém kontextu této práce síťové protokoly na jednotlivých vrstvách referenčních modelů, o kterých blíže hovoří část Výběr protokolů a hlaviček. "Nosič, který je zneužit pro přenos dodatečné (tajné) zprávy, se nazývá **cover** medium (či pouze cover)." [4]

"Pod termínem **sten**o**gram** chápeme, jak intuice napovídá, výskyt tajné zprávy (instanci coveru), v níž je ukryta tajná zpráva. Maximální velikost tajné zprávy, kterou lze daným stegosystémem do konkrétního coveru vměstnat, se nazývá steganografická kapacita tohoto coveru." [4] Tímto pojmem se obvykle označuje zpráva adresáta nebo příjemce, neboť musí být jasné, že tajnou informaci skutečně obsahuje, jinak by nemohl být nazván steganogramem.

V této diplomové práci se často potkávají také pojmy data a informace. Jejich význam je odlišný, nicméně v běžné řeči se používají oba dva bez výrazného rozdělení. Je vhodné uvést oba pojmy na správnou míru a přibrat i další – znalost. [5]



Obrázek 1.3: *Hierarchie pojmů*

Data jsou údaje popisující jevy, nicméně jejich samostatná užitečnost je nulová, pokud nejsou dána do souvislostí. **Informace** jsou interpretací dat v konkrétních souvislostech, poskytují tedy užitečný obsah z podstaty pojmu. **Znalost** je zastřešující schopnost interpretovat data a získat tak informace.

Při steganografii máme tajnou informaci, kterou tak doručujeme ve formě dat. Výzvou tvorby skrytého kanálu je provést zamaskování nejen posíláné informace, ale také zneviditelnění přenosu dat obsahující onu informaci.

1.3 Teoretický model

Obecný model pro aplikace steganografie popisuje mnohokráte citovaný myšlenkový experiment Gustavuse Simmonse pojmenovaný Věžňův problém s podprahovým kanálem (v originále The Prisoner's Problem and the Subliminal Channel) [6]. *(nezaměnit s vězňovým dilematem)*. Tato analogie dvou spolupachatelů držených ve dvou oddělených celách, kdy jediná možnost domluvy jejich společného útěku je přes dozorce, který představuje nespolehlivý prvek (ve smyslu autenticity) uprostřed komunikace, se stal základním teoretickým modelem steganografie.

Obrázek 1.4: *Formování plánu útěku skrytým dozorovaných kanálem [7]*

Ve své podstatě jde o to, jak v obecné a později i technické rovině zajistit, že skrytá komunikace mezi subjekty je korektně doručována, není modifikována (je autentická), není podvržená či zadržována a byla doručena v původním pořadí. Respektive obecněji je zajištěna autentizace, integrita, důvěrnost a nepopiratelnost.

Jedním z dalších základních myšlenkových experimentů u této problematiky je **Problém dvou armád**, někdy také Problém dvou generálů [8], který dokazuje nemožnost dvou subjektů shodnout se s jistotou přes nespolehlivé médium. Oproti předchozí výzvě s utajením jde v tomto případě o schopnost vůbec zprávu doručit.

Steganografie ve své ryzí podobě v rovině obecných modelů bez kryptografie připomíná obecný bezpečnostní model **Security through obscurity**. Jeho podstatou je utajení vnitřních mechanismů, čímž se zajišťuje důvěra v něj. Již dlouhou dobu, resp. od počátku, je takový princip považovaný za překonaný až nebezpečný, protože pouhé uniknutí informace o mechanismu ochrany narušuje bezpečnost v celém systému.

Mohlo by se nabízet zjednodušení, že tyto dva principy jsou identické, nicméně steganografie přenáší zprávu, pokud možno bez povšimnutí auditorem zabalenou do jiného nosiče a její prolamování je záležitostí konkrétního protiútoku. Bezpečnost skrze utajení přenáší zjevnou zprávu chráněnou nějakým druhem tajemství. Z vnitřního pohledu tak jde o protiklady, co a jak chráníme.

Tabulka 1.1: *Tabulka porovnání principů*

	Steganografie	**Bezpečnost skrze utajení**
chráněný objekt	zpráva	tajemství
prostředek k ochraně	tajemství	zpráva

1.4 Existující aplikace

Je zřejmé, že pokud bylo využití steganografie úspěšné, pak se o něm neví a lze předjímat, že tento princip musel být zveřejněn samotným odesilatelem či příjemcem. Z historie je známo mnoho netriviálních aplikací, pro ilustraci následuje osobní výběr zajímavých použití.

Nevynechatelný příběh každé publikace je případ řeckého Histiaiose, který vytetoval zprávu oholenému poslovi na hlavu, a poté počkal s jeho odesláním skrz nepřátelské území do doby, než mu vlasy opět dorostly. Příjemce posla opět oholil a zprávu přečetl. *Funkční, na dnešní dobu však neúměrně pomalé.*

Je známo i mnoho dalších případů [3] skrývaných zpráv na předmětech, byly jimi například "text pod voskem na prázdných psacích destičkách", "**tajné inkousty** na bázi ovocné šťávy nebo mléka, které jsou na papíře neviditelné, při zahřátí však zhnědnou". Dále také "zpráva na hedvábí zalitá do voskové kuličky, kterou posel polkl", v 16. století se objevil pokročilý příklad technické steganografie v podobě inkoustu na bázi roztoku kamence a skalice, kterým se zpráva napsala na vejce, a to se vzápětí uvařilo na tvrdo. Zpráva pronikla skořápkou na bílek, který se stal po oloupání vajíčka čitelný.

Jiným oborem jsou steganogramy lingvistické, které využívají obsahu textů. Jejich výhodou je možnost sdílení veřejným kanálem, neboť jejich viditelná část má obvykle svůj význam v přirozeném jazyce, který odvede pozornost. Nevýhodou je vyšší či přímo extrémní náročnost při vytváření, neboť vyžaduje až umělecký přístup k tvorbě steganogramu. Tato metoda (null ciphers) byla používána také v moderních dějinách, zejména ve zprávách špionů během světových válek a konfliktů. Rovněž byla důležitá při rozhlasovém vysílání na okupovaných územích.

My friend Bob, until yesterday I was using binoculars for stargazing. Today, I decided to try my new telescope. The galaxies in Leo and Ursa Major were unbelievable! Next, I plan to check out some nebulas and then prepare to take a few snapshots of the new comet. Although I am satisfied with the telescope, I think I need to purchase light pollution filters to block the xenon lights from a nearby highway to improve the quality of my pictures. Cheers, Alice.

mfbuyiwubfstidttmnttgilaumwuniptcosnatpttafsotncaiaswttitintplpft btxlfanhtitqompca

$$\pi = 3.141592653589793\ldots$$

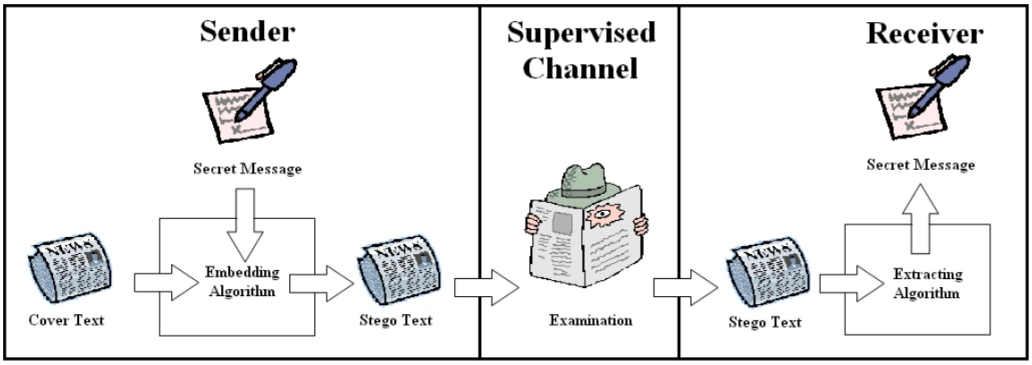
buubdlupnpsspx
attack tomorrow

Obrázek 1.5: *Příklad lingvistické steganografie používající dvojitý klíč [9]*

Zájemcům lze rovněž doporučit příběh Velvalee Dickinson [10], americké obchodnice s hračkami, která si korespondovala se zájemci o opravu poškozených panenek. V dopisech odposlechnutými FBI se však poškození figurek shodovalo se škodami na amerických válečných lodích za druhé světové války. Velvalee byla později dopadena, usvědčena a odsouzena.

Přístupy k vytváření jazykové steganografie v prostém textu mohou být různé – například **jinotaj** (z výše uvedeného příkladu). Všeobecně to však mohou být **n-tá písmena** ve slovech v rámci

věty (obr. 1.5), nebo nadpisech v rámci publikací, či jinak domluvený systém. Taktéž je možné ukrývat text použitím gramatiky "například v angličtině před slovem *and* může a nemusí být čárka. Výskyt čárky pak kóduje 0 nebo 1. Nevýhodou této metody je poměrně malá přenosová kapacita skrytého kanálu v poměru s objemem dat pro uložení zprávy." [11]



Obrázek 1.6: *Ilustrace principu šíření zprávy [9]*

S jazykovou steganografií souvisí také textová technická steganografie, která používá náhradu některých znaků v otevřeném textu určitého datového typu člověku jinými podobně vypadajícími znaky, které nesou data, či změnu **formátování** znaků obsahujících zprávu – zkosením, prokládáním, posunutím, použitým typem písma a jeho barvou nebo jiné **grafické** úpravy originálního textu.

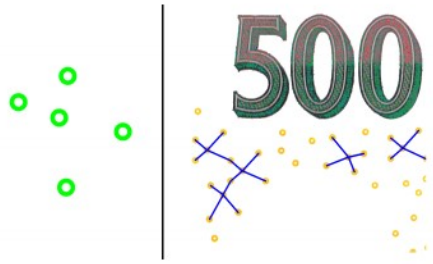
Je možné **nahrazovat** znaky podobnými jako O za 0, l za 1 či I, B za 8, E za 3, S za 5 apod. Mimochodem tento útok na grafické ztvárnění fontů řeší soubor znaků FE-Schrift (z německého překladu padělání znesnadňující písmo), kdy typickou aplikací jsou registrační značky vozidel.

Jinou variantou nahrazování jsou bílé znaky – velmi typicky například mezera, nezlomitelná mezera, pevná mezera či tabulátor. Tyto sekvence se zakódovanou informací se mohou snadno připojovat na konec textu, kde nejsou lidským okem viditelné, nebo využívají přirozené mezery mezi slovy.

Další technikou je přenos pomocí **mikroteček**, jehož podstatou je zmenšení dat obsahujících tajnou informaci do velikosti diakritických a interpunkčních znamének, které jsou posléze umístěny do veřejného otevřeného textu. Použití této techniky umožnil rozvoj vhodné technologie časově spadající do období od první světové války.

Obdobou mikroteček z předchozího odstavce a opětovným přiblížením k tématu steganografie jsou **žluté tečky** v barevných tiskárnách [12] obsahující časovou značku a sériové číslo pro usnadnění dohledání zdroje výtisku. Jde spíše o techniku vodoznaku, což je sesterská disciplína steganografie (viz Dělení principů), nicméně nám ukazuje, jak můžeme být i v současnosti obklopeni skrytými zprávami na nečekaných místech.

Příkladem skrytého vodoznaku je i EURion konstelace [13] neboli ochranný prvek bankovek, který zamezuje reprodukci platidel skenery, kopírkami a jejich úpravou v některých grafických editorech. Respektive při rozpoznání tohoto prvku je softwarem přerušena probíhající operace. Tato ochrana však není příliš účinná, neboť závisí na detekování obrazce, a rovněž musí být implementována v obslužném softwaru. Praktickým zjištěním v této oblasti bylo, že tisk této práce na ilustračním obrázku 1.7 skutečně selhal, k nápravě bylo potřeba změnit kompresní formát zdrojového souboru.



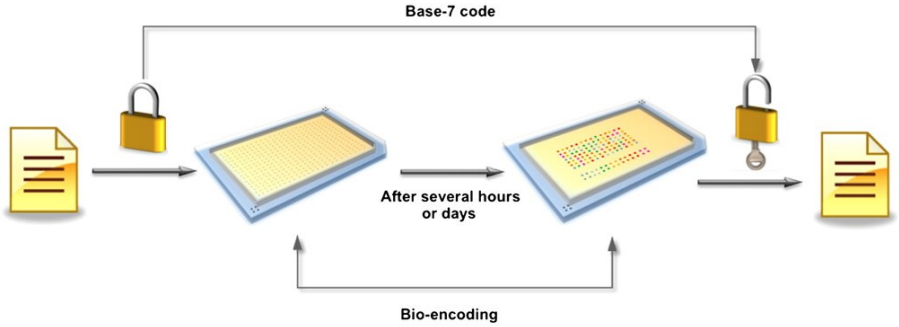
Obrázek 1.7: *Vlevo EURion konstelace, vpravo ukázka na části 500 Kč. [14]*

Mezi velmi mladé ukázky steganografie patří pořizování snímků obrazovky z počítačové hry World of Worldcraft [23], kdy se ve výsledném souboru fotografie objevily skryté informace o uživatelském jméně, herní postavě a o identifikaci herního serveru. Herní studio Blizzard chtělo tímto krokem zamezovat porušování licenčních podmínek a zjednodušit si pátrání po provinilých hráčích a ilegálních herních serverech.

Do oboru steganografie zařazujeme i podprahové signály, které jsou sdělovány "osobám pod limitem jejích vnímání, takže zprávu daná osoba sice zaregistruje, ale v té chvíli si ji neuvědomí, protože obsah signálu jí přejde přímo do podvědomí. Typicky je podprahovým signálem obrázek, který osoba vidí příliš krátkou dobu, aby došlo k vědomému rozpoznání, přesto lidský mozek výskyt zpracovává." [12] Známé, avšak zakázané, použití je v televizních reklamách.

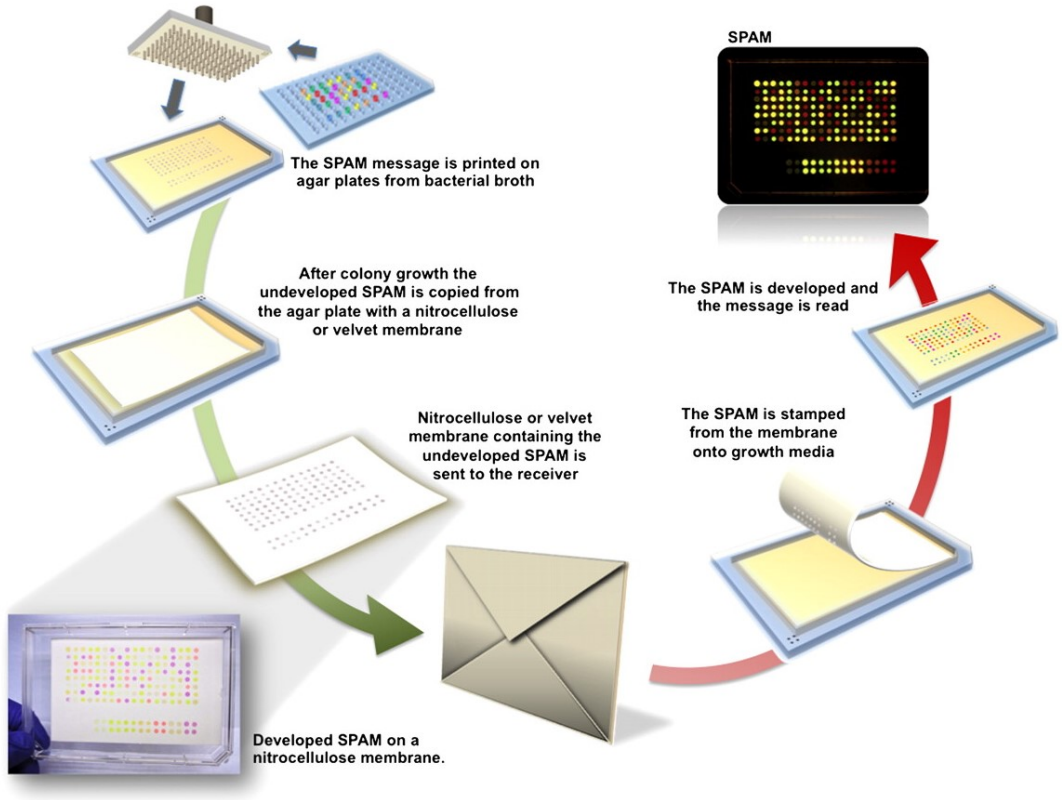
Původní myšlenka utajení přenosu vedla k objevení techniky frekvenčních skoků v rozprostřeném spektru (FHSS). Princip pro přístup k fyzickému médiu spočívá v pravidelném přeskakování mezi několika frekvencemi při přenosu bitů, pokud by došlo ke krátkému zarušení, je příslušný segment vysílaných dat přenesen na jiné frekvenci. Tato myšlenka se uplatnila při navádění torpéd [24] a stala se součástí 802.11 standardů. Prakticky stejnou logiku používá komerční WAN technologie ultra úzkého pásma nazývaná SigFox.

Mezi nejmladší výskyty steganografie řadíme ty, které probíhají biologickým přenosem. Výzkumníkům z Tufts University [15] se podařilo zakódovat data do mutované bakterie Escherichia Coli, která může mít až 7 rozdílných kmenů s odlišnými fluorescenčními vlastnostmi.



Obrázek 1.8: *Princip biologického přenosu [15]*

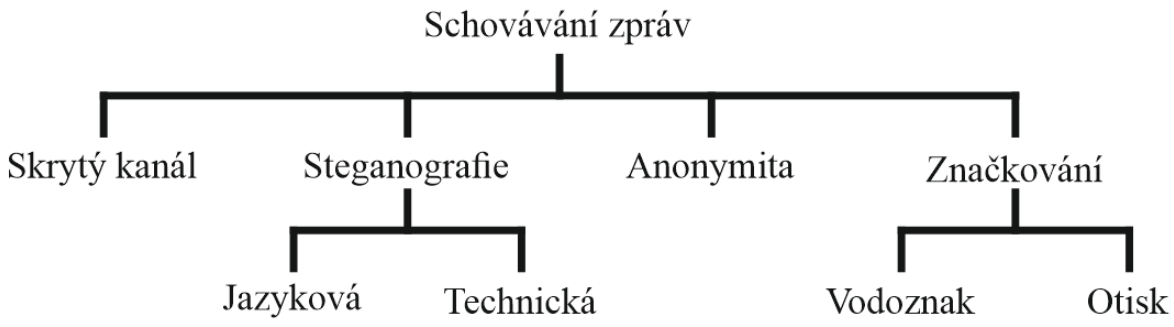
Nejprve se rozmnoží bakterie příslušných barev, které jsou naneseny do mikrotitrační destičky ve schématu zakódované zprávy. Poté se multikanálovou pipetou přenesou malé vzorky na agarovou kultivační destičku, odkud jsou po růstu dosud nerozvinutých kolonií umístěny na transportní médium jako nitrocelulózovou membránu či papír. Následuje přeprava k příjemci, který si médium umístí opět na kultivační destičku, zprávu vypěstuje, dekóduje a přečte.



Obrázek 1.9: *Proces biologického přenosu dat [15]*

1.5 Dělení principů

V praxi můžeme sledovat různá dělení steganografických technik [18] podle využívání odlišných principů, nebo jejich kombinací. Protože pojem steganografie zahrnuje mnoho médií (audio, video, obrázky, texty, soubory, …), je vhodné rozčlenit si je do následujícího stromu.



Obrázek 1.10: *Rozdělení technik skrývající informace*

Skryté kanály jsou takové způsoby přenosu, které nebyly v původním návrhu komunikační cesty zamýšleny. Ve své podstatě nejde o přímou steganografii, neboť zneužití technického prostředku je většinou viditelné. Mezi příklady patří například DNS tunnel.

Podstatou **steganografie** je vložení dat do jiných dat takovým způsobem, že úpravu je obtížné, ne-li nemožné vysledovat. Rozlišujeme variantu lingvistickou (jazykovědnou), jejíž podstatou je použití chytrosti v použitých slovech či slovosledu, a pak technickou, která vkládá surová data do prostorů v souborových a jiných formátech (zjednodušeně).

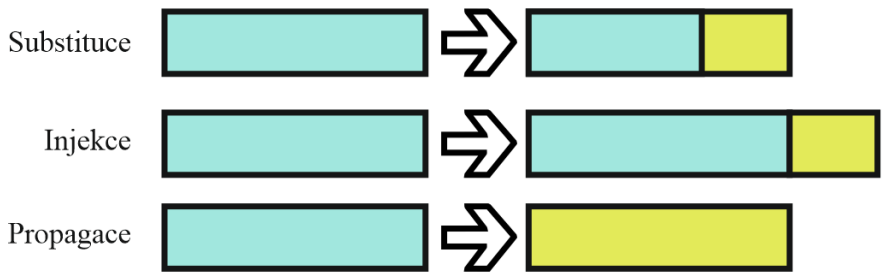
Principem **anonymity** je ukrytí odesílatele a příjemce, ale samotná zpráva není utajována. K dosažení cíle se používá zřetězený systém prostředníků, kteří si důvěřují.

Specifickou oblastí je **vlastnické značkování** (copyright marking), kdy jedním z cílů může být vložení neodstranitelného prvku do původního obsahu pro zajišťování autorských práv.

Dále budeme rozebírat technickou steganografii pro použití v síťovém modelu ISO/OSI, ke kterému se váží pojmy rozebrané v následujících odstavcích.

Steganograficky skrytý (a v určitých případech také postranní) kanál lze přenášet mnoha způsoby. Základním rozdělením je uložení informace buď **do datagramů**, nebo do **časové závislosti** mezi přenášenými zprávami.

V případě uložení do datagramů lze blíže rozdělovat, zda je zpráva umístěna **náhradou** (substitucí) místo některé z jedné či více hlaviček nebo je **vloženo** jinak prázdné pole (injekce). Poté lze uvažovat umístění informace do **prostoru užitečných dat**, kde lze získat místo rozdělením obsahu (fragmentací), či zmenšením původní informace (kompresí), nebo úplnou simulací přenosu, kdy jsou přenášená data kompletně nahrazena steganografickými (propagační steganografie) *(v tomto případě může být zavádějící pracovat s termínem užitečná data – anglicky payload)*.



Obrázek 1.11: *Příklady možných způsobů využití daného prostoru ve zprávě*

Samotná tajná data mohou být přenášena více způsoby. Nejzákladnějším je využití reálných hodnot (absolutních), které jsou vyčteny a dále zpracovány. Jiným přístupem může být modifikace existujících hodnot matematickými operacemi (relativně). Poslední možností je využití slovníků a kódových knih při přenosu informace.

Data lze také přenášet pomocí **časové domény**. Lze k tomu využít změny přenosové rychlosti, časování sekvencí, ztrát packetů, retransmise nebo úpravy pořadí doručení. [16]

Při rozdělení zohledňujeme i distribuci signálu, kterou může být jeden či více kanálů. Zejména při paralelní distribuci se odhalování zpráv stává složitější, neboť zachytit jednotlivé signály může být náročnější, zejména pokud se šíří odlišnými technologiemi.

Shrnutí: V literatuře [17], [4] se setkáme s obecnějším rozdělením steganografie na injektivní (vkládací), substituční (nahrazovací) a propagační (generující). Injektivní přístup vkládá do existujícího souboru tajnou zprávu, takže jeho výsledná velikost je větší, protože originální data si

zachovávají svou velikost. Substituční metody naopak nahrazují původní informaci steganografickou, takže výsledná velikost výstupu je identická s originálem na úkor kvality zdrojových dat. Propagační steganografie " nejčastěji využívá prostředky generující jiná data, která slouží jako krycí data. Vložená data jsou potom součástí těchto dat." [18]

1.6 Využití skrytých kanálů

Motivací, proč se zabývat steganografií, existuje velké množství. Asi nejzákladnější rozdělení zahrnuje dvě oblasti, a to legitimní a nezákonné aktivity, nicméně této práci nepřísluší posuzovat aktivity z právního hlediska, ponechává si tak odstup nutný pro technickou analýzu.

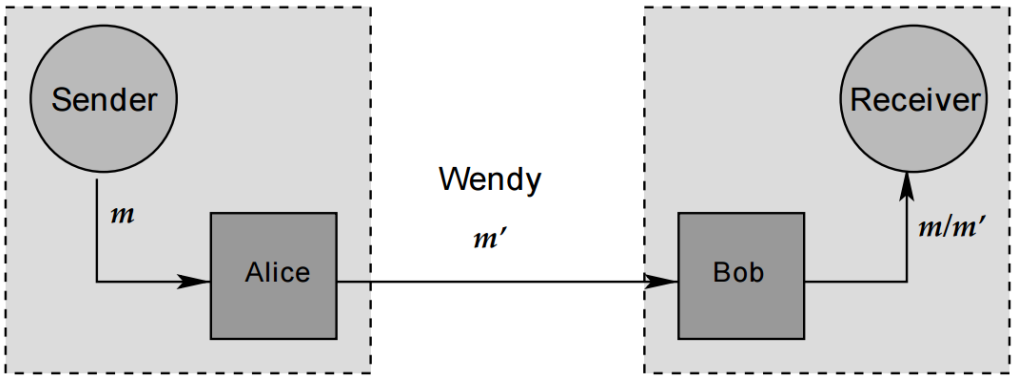
Některé z důvodů: [19] [20]

- komunikace mezi subjekty, které spolu nesmí komunikovat
- vynesení dat z chráněného prostředí
- instalace škodlivého kódu, ovládání botnetů
- vyhýbání se odhalení nepovoleného přístupu
- obcházení firewallů a filtrů při přístupu do zakázaných sítí
- vyvolání skrytých alarmů (například v Honeypotech) [21]

Spojujícím faktorem je snaha o nepozorovanou komunikaci z/přes/do střeženého prostoru. S rostoucím využíváním síťové komunikace roste s nejméně lineární úměrností datový provoz, jehož inspekce se stává náročnou, čímž se odhalování steganografie stává náročným.

1.7 Role objektů

V triviálním příkladu používajícím příměr vězení spolu komunikuje Alice (A) s Bobem (B) za dohledu dozorce (značen W v anglickém překladu Warden a odtud Wendy). Snažíme se však vyhýbat termínu man-in-middle, protože tento termín intuitivně implikuje jinou architekturu napadení komunikace, kdy podvržené datagramy vytváří prostředník, zatímco v našem případě typicky vystupují jako útočníci Alice s Bobem, ať už vědomě nebo ne.



Obrázek 1.12: *Schématické rozložení účastníků [22]*

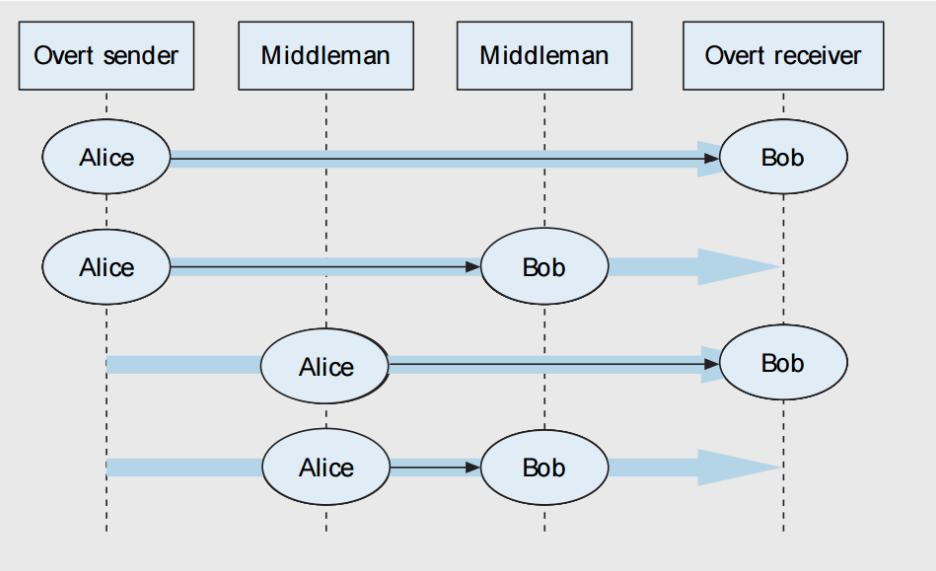
Zaměřme se na roli **dozorce** (taktéž auditor), tedy prvku, který se snaží probíhající steganografii rozpoznat. Můžeme jej klasifikovat jako pasivního, aktivního či zlomyslného.

Netečný dozorce provoz monitoruje, hledá skryté kanály, ale nezasahuje do nich, jen reportuje či provádí jinou úlohu upozorňování. Aktivní dohled nakažené zprávy zachytává a buď je opravuje

a posílá dál, nebo trvale zadržuje, z dlouhodobého hlediska se však chová konzistentně a deterministicky. Poslední zlomyslný dozorce je nejméně odhadnutelný, kombinuje oba principy pasivního i aktivního přístupu. Dozorce může zprávy i sám vytvářet bez vědomí odesilatele, a je třeba s ním počítat v návrhu skrytého kanálu, respektive v jeho robustnosti. Podle některých zdrojů [20] se však škodolibý dozorce příliš četně nevyskytuje.

Konkrétně technicky považujeme za auditora firewall, IDS (systém pro odhalení průniku), či IPS (systém prevence proniknutí), obsahový filtr, či jiný detekční systém.

Můžeme také rozebrat role Alice a Boba, které mohou být pojaty jak v roli nevinné oběti, tak i z pozice plného či parazitujícího útočníka, jak popisuje následující schéma.



Obrázek 1.13: *Přenos zprávy mezi objekty. Černá šipka značí skrytý kanál, modrá legitimní provoz [22]*

Z výše uvedeného obrázku vyplývá, že rozlišujeme veřejný legitimní kanál a skrytý steganografický proud dat. V prvním případě jsou koncovými body samotní autoři skryté zprávy. Tzn. mají pod kontrolou kompletní přenos.

V posledním případě je odesilatel i příjemce mezičlánkem (připomínající tunelující službu) a jejich úkolem je modifikovat procházející provoz s injekcí, substitucí či propagací (viz sekce Dělení principů) steganografických dat. Prostřední varianty popisují stav, kdy jeden z komunikujících objektů je plně pod kontrolou a druhý vystupuje v roli proxy serveru, který odebírá skrytou informaci a přeposílá data dále jako běžný provoz. Hodí se připomenout, že v tomto schématu není znázorněn dozorce provozu. Klíčový úkol před vlastní realizací některého z popsaných řešení nebo přípravou obranného mechanismu je uvědomit si, že zdrojem provozu nemusí být Alice ani Bob, ale může to být legitimně komunikující objekt, na kterém jenom prostředníci parazitují. Je třeba být mít toto na paměti při inspekci provozu v každé místě sítě.

2 Výběr protokolů a hlaviček

V této části budeme konkrétně rozebírat některé z vrstev referenčního modelu ISO/OSI a jednotlivé protokoly vhodné pro přenos informací. Nelze se však vyhnout připomenutí pojmů z počítačových sítí, protože jsou přímo propojeny s řešenou problematikou.

2.1 Orientace v problematice

Základní charakteristika jakýchkoliv síťových úloh se děje podle rozdělení do vrstev, které mají své konkrétní role rozděleny podle příslušného referenčního modelu, o kterých bude později hovořeno. Hodí se je však blíže uvést, protože jejich existence je poněkud abstraktní.

Nejčastějším přirovnáním je ilustrace dvou firem z odlišných zemí, mluvících odlišným jazykem, posílajících si nějakou obchodní zprávu. Původcem bude nejspíše ředitel společnosti píšící jiném řediteli dopis. Odesilatel nadiktuje své sekretářce text k překladu do jazyka příjemce. Ta jej předá asistentovi k přepisu na dopisní papír a předání na poštu. Po doručení zprávy příjemci je proveden stejný postup v opačném pořadí, tedy od setřídění asistentem, předání sekretářce a přečetní ředitelem. V případě odpovědi je proces proveden opět v původním pořadí. Smyslem příkladu je osvětlit, že jednotlivé komunikující objekty (vrstvy) si rozumí mezi sebou, ale nerozumí práci vrstvě pod sebou ani nad sebou (ředitel-ředitel, sekretářka-sekretářka, asistent-asistent). Stejným způsobem byly navrženy referenční modely.

2.1.1 Referenční model ISO/OSI

Tabulka 2.1: *Přehled jednotlivých vrstev modelu referenčního modelu*

Číslo vrstvy	Jméno vrstvy	Název datagramu	Směr průchodu do zařízení
1	Fyzická	Bity	↓
2	Spojová	Rámec	
3	Síťová	Paket	
4	Transportní	Segment	
5	Relační	Protocol Data Unit	
6	Prezentační	PDU	
7	Aplikační	PDU	
-	-	datagram	obecný pojem pro kteroukoliv z vrstev

Referenční model je sedmivrstvé logické rozdělení úloh zpracování síťového provozu. Jednotlivé vrstvy jsou dále rozebírány v textu. Podstatou je nezávislost a nahraditelnost implementace jednotlivých úrovní například při změnách technologie z drátového Ethernetu na Wi-Fi apod.

Klíčové pro tuto práci jsou především názvy uvedených datagramů, neboť v teoretickém i reálném prostředí jsou jimi konkrétně vymezeny uvedené vrstvy, které se váží na konkrétní protokoly.

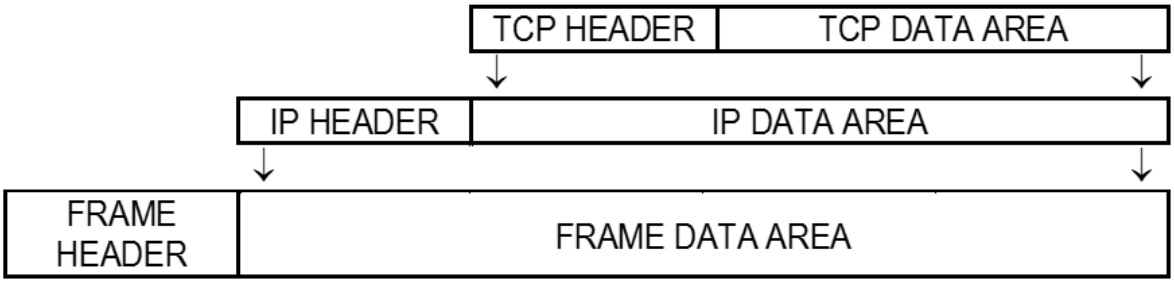
Alternativou referenčního modelu ISO/OSI je model TCP/IP, který zjednodušuje soustavu do 4 vrstev v obdobných funkcích. Důvody pro toto odlišení vycházejí z historie návrhů modelů a na zajišťování spojovaného nebo nespojovaného spojení v rámci některých vrstev. [25] Nicméně model TCP/IP, ačkoliv je kompatibilní, se pro potřeby této práce hodí méně a není dál používán, je však uveden pro kompletnost. Navíc převoditelnost na tento model je snazší než v opačném směru.

Tabulka 2.2: *Porovnání a přirovnání jednotlivých vrstev modelů*

TCP/IP model	**ISO/OSI model**
Fyzická	Fyzická
	Spojová
Síťová	Síťová
Transportní	Transportní
Aplikační	Relační
	Prezentační
	Aplikační

2.1.2 Zapouzdření a zpracování při průchodu

Zapouzdření (enkapsulace) je přístup, který odděluje obsah každé vrstvy od obsahu vrstvy předcházející a také následující. Princip vychází z prefixování a postfixování hlaviček daného protokolu před a za datovou oblast, přičemž datovou oblastí se rozumí celý obsah každé předcházející vrstvy. Výstižněji zobrazuje problematiku následující schéma:



Obrázek 2.1: *Schématické znázornění vrstev a hlaviček na 2., 3. a 4. vrstvě při pohledu zespodu. [26]*

Výsledným efektem je kaskáda vnořených dat, o které se aktuální vrstva nezajímá, protože zpracovává pouze své hlavičky, nicméně po postoupení vnořených dat do další vrstvy se tato data rozbalují a opět je na ně nahlíženo jako na hlavičky a obsah. Steganografická data se pak v rámci jednoho skrytého kanálu mohou nacházet na více vrstvách současně.

2.2 Výběr protokolů

Při výběru protokolů vhodných pro steganografii bylo nutné řídit se zadáním, které vymezuje použití na 3. až 7. vrstvu. Zde se hodí okomentovat, že takové omezení má zřetelný důvod ve specifikaci průchodnosti steganografické zprávy Internetem, respektive přesněji je taková zpráva průchozí mezi sítěmi a není omezena na jeden síťový segment v rámci stejného adresního rozsahu. Z výše uvedeného popisu síťového modelu ISO/OSI tak musíme vyloučit protokoly první (fyzické) a druhé (spojové) vrstvy referenčního modelu ISO/OSI, které na hranicích lokálních sítí ztrácejí svá záhlaví a jsou nahrazovány novými záhlavími, logicky tedy do nich nelze ukrývat žádná data při přenosu mezi sítěmi.

Tato práce si dala za cíl analyzovat především situaci ve stabilním nosném protokolu IP verze 4 používajícím 32 bitové adresy síťových uzlů. Díky starší koncepci návrhu obsahuje tato varianta množství redundantních polích v hlavičkách, která se dají využít kromě původního záměru také pro steganografické účely. Internetový protokol ve verzi 4 je v současnosti stále majoritně používán pro přenos datagramů v počítačových sítích.

Nástupcem verze 4 je verze 6, která pracuje se 128 bitovými adresami síťových uzlů. Ke steganografii při jejím použití je třeba přistupovat odlišně, neboť byl v návrhu omezen počet pevných polí záhlaví. V této práci jsem se síťovým provozem používajícím protokoly verze 6 nezabýval.

2.2.1 Síťová vrstva

Síťová vrstva je skupina protokolů, metod a specifikací, které jsou využívány při přenosu paketů od síťového zdroje k adresátovi přes síťové hranice, pokud je potřeba. Děje se tak na základě síťové adresy, provoz je směrován nezávisle na ostatních paketech bez předem sestaveného spojení.

2.2.1.1 Protokol IP

Je to bezokruhový paketově orientovaný protokol operující v režimu nejlepšího úsilí, které nezaručuje spolehlivé doručení datagramu, negarantuje stejné pořadí doručení a nevylučuje možnost duplikací. Zmíněné nedostatky a i další jsou předmětem případného dodatečného dohledu vyšší Transportní vrstva. Základní funkcí protokolu IP je směrování paketů od zdroje k cíli přes jednu nebo více sítí. Při steganografii v této oblasti je třeba se zmíněnými vlastnostmi počítat a nespoléhat se na "nejlepší úsilí", které však většinou poskytuje

2.2.1.2 Protokol ICMP

Internet Control Message Protocol je podpůrným protokolem využívaným síťovými zařízeními k předávání si chybových a jiných hlášení. Svým návrhem se odlišuje od ostatních protokolů transportní vrstvy tím, že není určen k zasílání užitečných dat, ale pouze služebních informací. Kromě několika výjimek (ping, tracert, …) není používán koncovým uživatelem.

Zprávy tohoto protokolu se vytváření nad IP vrstvou, ačkoliv se stále považují za součást 3. vrstvy referenčního modelu ISO/OSI. Obvykle z IP datagramu, který ICMP reakci vyvolal. Síťová vrstva patřičnou ICMP zprávu zapouzdří novou IP hlavičkou (aby se ICMP zpráva dostala zpět k původnímu odesílateli) a obvyklým způsobem vzniklý datagram odešle.

2.2.2 Transportní vrstva

Transportní vrstva určuje způsob zajišťování spolehlivosti doručení segmentů předchozí úrovně a provádí tak finální službu koncovým uzlům síťového spojení.

2.2.2.1 Protokol UDP

Jedná se o bezspojový jednoduchý mechanismus pro posílání segmentů s kontrolními součty pro datovou integritu. Poskytuje adresování porty pro rozlišování služeb, nicméně neobsahuje garanci doručení, pořadí či duplikace jako protokol TCP. Kontrolu a zacházení s chybami je třeba řešit na vyšší úrovni.

Takový model síťového provozu se hodí pro vysokorychlostní objemné přenosy většinou v reálném čase, kde nezáleží na malých ztrátách, ale prioritou je včasné doručení dat s minimalizací zpoždění. Ze stejného důvodu pak zadání této diplomové práce neumožňuje tento způsob přenosu používat, protože v datových tocích internetových sítí je steganografie do velkého objemu dat malou výzkumnou výzvou.

2.2.2.2 Protokol TCP

Transport Control Protocol (TCP) se používá pro spolehlivé doručování segmentů přes nespolehlivou síť v pořadí jejich odeslání. Prakticky je tedy několika mechanismy dbáno o přijetí všech odeslaných zpráv a v případě výpadku také o opětovné zaslání chybějících částí přes nižší IP vrstvu. Majorita internetových služeb (webové stránky, email, přenos souborů, …) používá tento typ přenosu, protože jednotlivé aplikace jsou od sebe odlišeny používáním čísly portů.

2.2.3 Relační vrstva

Smyslem páté vrstvy, **pokud je využita**, je řídit a udržovat dialog mezi komunikujícími stranami uživatelských procesů zejména v prostředích, kde se využívá volání vzdálených procedur (RPC). Metody relační úrovně vstupují do komunikace, pokud je to nutné, například určováním strany vysílání, taktéž se starají o ukončování a rušení relací. Vrstva umožňuje informacím z odlišných datových proudů pocházejících z odlišných zdrojů, aby byly korektně zkombinovány nebo synchronizovány.

Zatímco nižší vrstvy (1. - 3.) přinášejí funkcionalitu nezbytnou pro samotnou komunikaci, úroveň čtvrtá pak izoluje konkrétní komunikační podsíť od samotných účastníků. Každá další rovina (5. - 7.) je orientována spíše na výpomoc síťovým aplikacím. Relační vrstva patří mezi nejméně využívané [29] z referenčního modelu ISO/OSI.

Ačkoliv prameny uvádějí různé protokoly relační (i následující prezentační) vrstvy, prakticky se nerozlišují [25] a intuitivně se přesouvají do úrovně aplikační, čímž více odpovídají referenčnímu modelu TCP/IP.

2.2.4 Prezentační vrstva

Tato úroveň se stará o datový překlad přenášených informací tak, aby reprezentace dat byla shodná pro oba systémy, jestliže komunikující strany používají jiný zápis hodnot například kódování znaků ASCII/UTF či vyjádření čísel. Pan Jiří Peterka [30] taktéž uvádí, že tato úroveň se stará o serializovatelnost dat, pokud jsou přenášena například vícerozměrná pole, přičemž se využívá abstraktní syntaxe jazyka ANS.1 či podobných.

Podstatné je také šifrování na této vrstvě, i když to není (a nemá být) jediný způsob zabezpečení. Z podstaty funkce se však tato činnost nejvíce vyhovuje právě v tomto místě.

2.2.5 Aplikační vrstva

Je to místo styku uživatelské aplikace s rozhraním komunikační sítě. Její součástí jsou entity jako prvky, které používají síť definovaným způsobem podle protokolů. Část, která je specifická pro každou aplikaci (uživatelské rozhraní) se za součást aplikační entity a vrstvy již nepovažuje.

2.2.5.1 Protokol DNS

Jedná se o způsob komunikace služby pro překlad lidsky přívětivých doménových jmen na numerické číselné adresy používané počítači pro směrování síťové provozu ke zdrojům a zpět. Bez jeho existence by byl současný internet nefunkční, patří tedy k elementárním prvkům internetového provozu, a proto se vyplatí se jím dále zabývat.

2.2.5.2 Protokol HTTP

Slouží k výměně textových a obohacených textových zpráv dokumentů přes síťové prostředí. Obsahuje taktéž rozšíření pro multimediální data. V současnosti jde o jeden z nejpoužívanějších protokolů na internetu, respektive pak jeho zabezpečená verze HTTPS.

2.2.5.3 Protokol SIP

Tato práce se blíže nezabývá telefonními protokoly služeb VoIP, protože téma je již dostatečně zpracováno katedrou telekomunikační techniky VŠB.

2.3 Výběr částí hlaviček

V následujícím bloku analyzujeme pole, která lze pro stenografické účely použít. Cílem v tomto hledání je identifikovat pole, která nejsou využívána, či je lze nějakým způsobem upravit bez toho, aby došlo k narušení funkcionality sítě. Vhodné je také hledat hodnoty, které jsou nějakým způsobem založeny na náhodnosti, jelikož tyto hodnoty lze snadno nahradit vlastními daty, které mohou vypadat náhodně.

2.3.1 Protokol IP

2.3.1.1 Type of service

Obsahuje 8 bitů pro určení kvality a priority přenášených dat. V dnešní době se tato položka většinou nevyužívá k původní funkci, takže je možné zde umístit steganografická data. V současnosti se pole využívají pro služby Differentiated services zajišťující kvalitu přenosu (QoS), ale tato služba není povinně využívána, proto je zde opět prostor pro steganografii. Bez dopadu na funkcionalitu je použití bitu 6 až 7, které jsou rezervovány pro budoucí použití.

2.3.1.2 Identification

Obsahuje 16 bitovou hodnotu jako identifikátor, který pomáhá při sestavování příchozích paketů. Pro každé unikátní spojení dané množinou odesílatel – příjemce – protokol se nastavuje jedinečná hodnota, který by měla být po nějaký čas unikátní (IETF doporučuje 2 minuty) [27]. Primární funkcí tohoto pole je usnadnit defragmentaci paketů, které při procesu rozdělování dostanou stejné ID, čímž usnadní opětovné sestavování.

Ze steganografického hlediska je náhodnost hodnoty tohoto pole žádoucí a lze do něj uschovat potřebné údaje. Novější revize tohoto pole v RFC 6864 zakazuje jakékoliv použití.

Tato pole se dají snadno využít jen v případě, kdy po trase nedochází k fragmentaci, případně lze využít příznaku Do Not fragment, kdy ale dochází k podezřelé kombinaci hodnot polí. Path MTU Discovery

2.3.1.3 Příznaky

Značky obsahující celkem 3 bity. První z nich "MF" značí, že došlo k fragmentaci, druhý "DF" zakazuje provedení fragmentace (don't fragment). Poslední, dosud nezmíněný, je tzv. Evil bit [28], který je kromě své zanedbatelné délky přímo podezřelý při využití, protože jeho standardní hodnota má být trvale nulová.

Steganografie v příznacích se nabízí využitím DF a Evil pole, kterým získáme 2 bity na každém packetu, ovšem za cenu snadné detekovatelnosti.

2.3.2 Protokol ICMP

Hlavičky se dělí na požadavky a odpovědi, ve společné části se nenachází prostor pro steganografii. Jelikož klient se dotazuje protistrany, odesílá zprávy ICMP Echo, ve kterých lze nalézt:

2.3.2.1 Identifier

Slouží k rozpoznání spojení podobně jako port v TCP vrstvě, čímž usnadňuje párování požadavků a odpovědí. Implementace je dle RFC ponechána na aplikaci, a proto je 16 bitová hodnota perfektní ke steganografii. Šance na odhalení je nižší, pokud se hodnota nemění v rámci jedné transakce (sérii dotazů).

2.3.2.2 Sekvenční číslo

Tato 16 bitová hodnota rovněž pomáhá identifikaci páru požadavku a odpovědi. V průběhu transakce dochází k inkrementaci hodnoty, proto je vhodné nastavit tuto hodnotu na začátku, a poté regulérně inkrementovat, čímž je splněn její legitimní účel.

2.3.3 Protokol TCP

2.3.3.1 Sekvenční číslo a potvrzovací číslo

Jsou 32 bitové hodnoty, které mají kritickou funkci v průběhu spojení, nicméně jejich inicializace je prováděná náhodnými daty, která je možno zaměnit za steganografická. Kapacita kanálu za pomocí těchto polí je malá, neboť změnu je možné provést jen s novým navázáním spojení, hodí se tak jako doplněk jiných metod. [32]

2.3.3.2 Options Timestamp

Význam časové značky spočívá především ve zlepšení výkonnosti TCP, obzvláště v případě ztrátovosti paketů. [32] Původně byla obsažena hodnota globálního času, což je považováno za bezpečností riziko, proto může být čítač pro jednotlivá TCP spojení unikátní a náhodný, což poskytuje prostor 32 bitů pro vložení vlastních dat.

2.3.3.3 Urgent pointer

Toto 16 bitové pole pro svůj regulérní účel využívá nastavení příznaku URG a společně slouží k upřednostňování takto označeného datagramu před ostatními v prioritě zpracování. Prakticky tato položka odkazující na konec prioritních dat není používána, proto je použití nápadné, i když poskytuje nezanedbatelný steganografický prostor. [36]

2.3.4 Protokol DNS

2.3.4.1 Identifier

Je 16 bitová náhodná hodnota, která spolu páruje dotaz z odpovědí. Dle zvyklostí jde o hodnotu inkrementovanou, nejde však o standard [37], nabízí proto prostor pro steganografii.

2.3.4.2 Dotazy a odpovědi

DNS protokol obsahuje zvláštní sekce v hlavičce podle způsobu užití jako dotazu či odpovědi. I ve formálně vypadajícím požadavku lze však zahrnout i část odpovědi [37], ve které je možné přenášet steganografická data bez vlivu na funkčnost DNS dotazu.

2.3.5 Protokol HTTP

Na této vrstvě lze nalézt největší množství prostoru pro steganografii, protože jde o nejrůznoroději používaný protokol v internetu.

Zde se výzkum nezaměřoval příliš do hloubky, bylo implementováno jen demonstrační řešení. Nabízí se zde využití množství hlaviček včetně nestandardních a experimentálních. Potenciálně je také možné použití šifrované verze, kde není čitelný přenášený obsah, ale ve své podstatě už nejde o steganografii.

2.3.5.1 Dotaz a odpověď

Mezi řešení, které je plně síťově transparentní a zároveň steganografické, patří uchování tajné informace v samotném GET požadavku, který obsahuje zdánlivě náhodné shluky znaků, typicky adresy obrazových souborů na sociálních sítí. Dále se nabízí rozšíření zpětného kanálu i pomocí zaslání nějaké odpovědi (v tomto případě typu MIME s obrázkem) která obsahuje další skrytý kanál, například krytý obrazovou steganografií.

3 Návrh a implementace skrytého kanálu

Doposud byly zmiňovány obecné nebo stroze technické informace, následující blok si dává za cíl rozhodnout, kdy a který aspekt bude využit k dosažení cíle.

3.1 Návrh skrytého kanálu

První a klíčovou otázkou je vlastní prostředí, ve kterém k steganografii dochází – jde o "super střežené armádní datacentrum" odpojené od internetu, a o jehož představě má veřejnost z populárních filmů (obrázek 1.15), nebo například separovanou oblast v síti soukromé korporace, ve které je drženo know-how se zpětnou inspekcí datového provozu, nebo je skrytým kanálem ovládán jiný počítač, jehož kontrola nemá být ztracena zablokováním pravidly na firewallu? Variací této otázky by se našlo mnoho, zároveň je naprosto primární při implementaci.

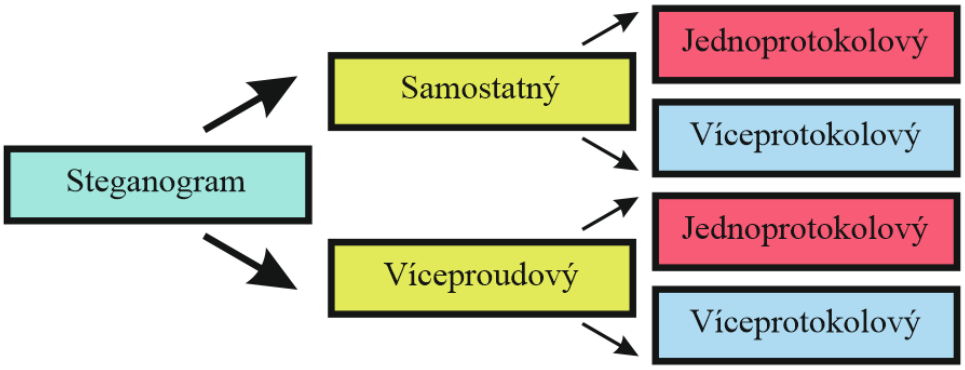
Další otázkou je vlastní forma dat k přenosu pro určení kódování do bitových polí záhlaví. Je esenciální vědět, jsou-li vstupní data bezztrátově převoditelná po částech do binární či jiné podoby, protože záhlaví nám poskytují prostor v řádech jednotek bitů. Jinou variantou mohou být celočíselné, většinou bezznaménkové datové typy, používané v některých hlavičkách, ale opět je potřeba přijít na způsob převodu datového zdroje do tohoto formátu a jeho rekonstrukci zpátky.

Při určení konkrétního prostředí se také otevírají požadavky na další technické parametry skrytého kanálu, například kapacita, spolehlivost či směr komunikace (jednosměrný či oboustranný) a ověření autenticity zprávy či dokonce autentizace členů přenosu. Ve své podstatě se návrhář potýká se všemi známými problémy návrhu komunikačního protokolu zvýšeného o problém jeho utajení.

3.1.1 Vrstvení

Pro ukrytí zprávy v datagramu je možné, ale ne nutné, použít více protokolů v rámci **téhož** datagramu. Výhodou použití jediného protokolu (například DNS) jako nosiče steganografie je snadnost implementace a s tím spojená kratší doba do nasazení. Nevýhodou je nižší přenosová kapacita nebo menší odolnost proti objevení.

Využíváním všech vrstev referenčního modelu je dosaženo vyšší kapacity. Skrytí steganografie je usnadněno, protože nižší vrstva je vždy přítomna z principu fungování sítě (například IP+UDP+DNS). Nevýhodou je vyšší složitost obsluhy kanálu ze softwarového pohledu a přídavné obtíže s opětovným sestavením, pokud dojde k dílčí ztrátě v přenosu.



Obrázek 3.1: *Stromový diagram klasifikace tvorby skrytého kanálu*

3.1.2 Proměnlivost

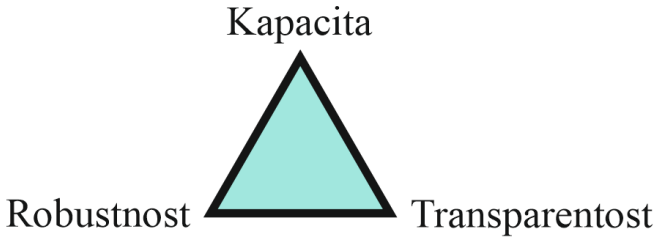
O neúspěšnosti steganografické komunikace může také rozhodnout, zdali se využívá stále stejného klíče pro ukrývání dat, nebo se ve svém chování mění v čase, či po určitém objemu odvysílaného obsahu.

Ideálně by se mělo využívat Kerckhoffsova principu, podle kterého by se bezpečnost neměla zakládat pouze na utajení principu jako v kryptografii [31]. Prakticky je takový cíl nedosažitelný už z pouhého principu, protože struktura datagramu je daná a prostoru pro ukrývání dat zde navíc není mnoho. Variabilitu lze však zajistit Vrstvení či rozdělením do více proudů a bezpečnost informace pak samostatně kryptograficky.

Zdaleka největší prostor k přenosu steganografického obsahu tak poskytuje co nejreálnější využívání kompletního síťového provozu neboli simulace či zásah do reálné služby. Prakticky to představuje například vyslání servisního dotazu na dostupnost uzlu, dotaz na překlad doménového jména, ovlivnění datagramů sestavení a samotného datového provozu. Ačkoliv tato úvaha se zdá být přirozená, její realizace není triviální, protože vyžaduje aplikaci pravidel nejen steganografických, ale také pravidel řízení síťového provozu.

3.1.3 Vyvážení

Niels Provos a Peter Honeyman v článku [3] definují tři aspekty hodnocení systémů pro ukrývání informace – kapacita, bezpečnost, robustnost. Jak vyplývá ze schématu 1.16, dosáhnout všech 3 vlastností je nemožné ve stejný čas a je třeba hledat funkční kompromis.



Obrázek 3.2: *Ternární diagram vyvážení vlastností skrytého kanálu*

„Existuje však jistá (nejasná) míra bitového objemu, kterou nesmí vkládaný objekt překročit, aby výsledný stegogram stále vypadal dostatečně nenápadně. Tento bitový objem zahrnuje jak samotnou utajovanou zprávu, tak režijní data stegosystému a redundanci, která zajistí robustnost.“ [3]

3.1.4 Robustnost

Protože přenos probíhá přes nespolehlivý kanál, je třeba zajistit vnitřním mechanismem odolnost proti výpadkům v doručení datagramů. Standardně tuto úlohu zajišťuje TCP a vyšší protokoly, které ovšem nemusí být využity. Může se vyskytnout také manuální implementace, která neprovádí službu spolehlivosti dle standardů či je kombinována s jinou steganografickou vrstvou, kdy opětovné vysílání sice poskytne utajená data transportní vrstvě, způsobí však zmatek v jiné typicky nižší části referenčního modelu. V těchto případech je třeba mít zajištěnou robustnost i na samotné vrstvě steganografické.

Zde se nabízí implementovat přídavnou logiku s redundancí uvnitř steganogramu, ovšem za cenu objemnějšího přenosu. V průběhu implementace se ukázalo, že průběžná detekce a žádosti o opětovné vysílání části steganogramu jsou algoritmicky náročné a zásadním způsobem komplikují čitelnost metod a orientaci v jejich zdrojovém kódu.

Proto bylo navrženo řešení, ve kterém se detekuje integrita přijaté zprávy – kompletnost a nepoškozenost při přenosu za pomocí režijních dat v steganografické zprávě, které jsou po kontrole vyjmuty a k příjemci zprávy nedorazí. V případě, že ověřovací metody hlásí problém, je i příjemce informován, že zpráva není v pořádku.

Jak se postupuje v případě chyby? Pokud je aktivován zpětný (obousměrný) kanál, je možné odesilatele informovat o chybě a žádat nové vysílání. Pakliže je využito jednosměrné předávání, měla by být odesilatelem zpráva vysílána nejméně dvakrát ke snížení rizika z možné chyby a porovnání výsledků, čímž se ale zvyšuje riziko odhalení. Při volbě tak záleží na mnoha aspektech konkrétního nasazení, nicméně situace se přibližuje do stavu úvahy o Problému dvou armád z kapitoly Teoretický model.

Standardními technikami k rozpoznání integrity zprávy v oboru je využití kontrolního součtu jako paritního bitu, zbytku při dělení (modulo), dále také cyklických kontrolních součtů či hašovacích funkcí viz tabulka 3.1. Klíčové je pro nás rozpoznání úplnosti a správnosti informace, kterým zabraňujeme modifikacím pocházejícím z chyb při přenosu a také z možného záměrné modifikace.

"U samodetekčních kódů je možné ověřit správnost dat, při odhalení chyby ale není možné zjistit původní informaci. Tento nedostatek je odstraněn u samoopravných kódů, které dovolují při dostatečně malém poškození zrekonstruovat původní data. V obou případech jsou dodatečné informace redundantní, tj. nepřenášejí užitečná data a tím pádem snižují efektivitu záznamu dat nebo přenosu." [34]

Tabulka 3.1: *Výběr metod pro kontrolu integrity přenesených dat*

Kód	Metoda	Varianta
Detekční	Paritní bit (kontrolní součet)	sudá/lichá
Detekční	Modulo (kontrolní součet)	%11
Detekční	Cyklický redundantní součet	CRC-32
Detekční	Hash funkce	MD5
Opravný	Hammingův kód	(7,4)
Opravný	BCH kód	q,m,δ

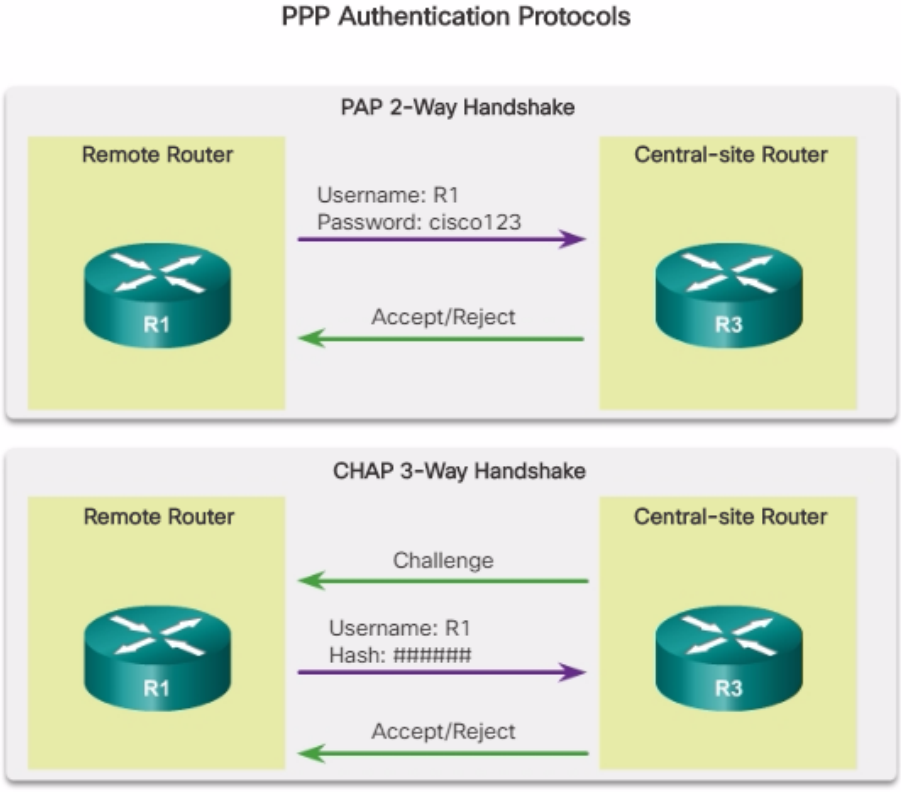
3.1.5 Sestavení spojení

Každé navázání steganografické komunikace by mělo být v souladu s pravidly protokolu, který je využíván jako hostitelský. Otázkou je, jak rozpoznat, že byl otevřen skrytý kanál, pokud přenosové médium není bez komunikace, nebo používáme port, na který může přijít i jiná komunikace.

V síťovém uspořádaní v tomto případě vyhovuje model, kdy jedna strana navazuje spojení (klient) a druhá vyčkává na spojení (server). Z podstaty steganografie vyplývá, že rozpoznání navázání modifikovaného spojení je možné jen v případě, kdy jej druhá strana očekává a zná jeho princip. Stejný princip se uplatňuje pro ukončení spojení, kdy je potřeba informovat o skutečnosti, že žádná další zpráva již nenásleduje.

První zpráva tedy musí obsahovat nějaký klíč, který druhá strana rozpozná a odpoví předepsaným způsobem jako reaguje každý jiný síťový protokol. Jelikož je snaha o minimalistickou komunikaci, je preferován nižší počet výměn sestavovacích zpráv. Lze také kopírovat postup hostícího protokolu, ale není to nezbytně nutné, či dokonce možné, pokud v něm k tomuto nedochází. V takovém případě pak stanice nemusí vyjednávat o komunikaci, protože se předpokládá, že tyto informace již v sobě mají předány postranním kanálem.

Při výzkumu v této oblasti byla snaha najít podobné principy a funkční modely v běžných síťových protokolech a exitujících modelech. Zde byla nalezena inspirace v **protokolu CHAP** s třícestnou výměnou úvodních zpráv, které jsou navíc spojeny s ověřením identity uživatele. Protokol je vylepšením původního protokolu PAP, kdy nepřenáší ověřovací tajemství v čitelné formě. Používá 3 cestné sestavení spojení a ověřování identity obvykle probíhá i v průběhu komunikace, což vyhovuje i případu steganografie.



Obrázek 3.3: *Schéma protokolu PAP a CHAP [35]*

Navazování komunikace je potřeba hlavně z důvodu rozlišení zpráv, ve kterých hledat skrytý obsah, protože zejména příchozí síťový provoz může pocházet z mnoha zdrojů. Na tyto požadavky by mělo být regulérně odpovídáno, čímž je v ideálním případě krytý skutečný účel serveru jako příjemce steganografických zpráv. Poskytováním regulérního obsahu na požadavek se tak kryjí před odhalením

i samotné zprávy obsahující steganografii. Prakticky se tedy implementaci této funkcionality nedá efektivně vyhnout.

3.1.6 Transparentnost

Klíčovou vlastností steganografie je být neviditelnou při vnějším pohledu, což v síťovém prostředí znamená, že nosič skrytého kanálu musí vypadat reálně, tedy zabezpečovat nějakou funkci, kterou lze v daném síťovém perimetru očekávat. Tato primární funkce síťové komunikace není podstatná pro přenos ukryté informace, ale je klíčová pro úspěšnost komunikace, neboť odhalením skrytého kanálu dochází k prozrazení použité techniky, kompromitaci zprávy, či dokonce její modifikaci a patrně v nejzávažnějším důsledku k odkrytí komunikujících subjektů – odesilatele a příjemce.

Aby k tomuto sledu událostí nedošlo, je potřeba důsledné krytí kanálu tím, že je dbáno o přirozenost vnější komunikace. To prakticky znamená, že není možno zahájit intenzivní dávkovou komunikaci servisního protokolu s doposud neznámým objektem v síti apod., protože dojde k vyvolání podezření. Jiný příklad – Při připojení nejen k podstrčenému webovému serveru dochází nejprve k dotazu na překlad doménového jména na IP adresu, poté k sestavení spojení, výměně dat a jejich potvrzování následované ukončením spojení. Logicky tedy nelze úspěšně, natož dlouhodobě, vytvořit steganografický kanál, který ze zmíněného postupu používá jen výměnu dat bez doplňkových transakcí.

Tvorba standardního toku pro steganografické účely se zdá být podobně obtížnou úlohou jako samotné umístění a přenos zprávy. Význam kvality, smyslu a transparentnosti v souladu se standardy u nosného kanálu pak roste společně s tím, jak úzkostlivě je střežen prostor, ve kterém k přenosu probíhá.

3.1.7 Prostředí

Jednou z nejpodstatnějších otázek oboru přenášení ukryté zprávy je po dostupnosti síťové komunikace a přístupu ke koncovému uzlu (klientovi) právě otázka tykající se autority dohlížející na síťový provoz. Nabízí se několik scénářů, jejichž některé praktické výskyty byly uvedeny v části Návrh a implementace skrytého kanálu. Klasifikace prostředí:

- bez dohledu
- se statickými pravidly (firewall)
- s dohledem (technický / lidský)
    - pasivním (IDS)
    - aktivním (IPS)

Stupeň ochrany se také v technické praxi liší podle síťového segmentu, ve kterém se uzel odesílající steganografii nachází a zda je součástí organizace zvláštní bezpečnostní tým CERT/CSIRT.

- zóna pracovních stanic
- zóna datacentra
- zóna návštěvníka
- demilitarizovaná zóna (DMZ)
- izolovaná zóna (Honeypot)

3.2 Implementace skrytého kanálu

3.2.1 Základní parametry

Pro konkrétní návrh síťové steganografie se využije z teoretického rozboru technika substituce při umisťování skrytých dat, protože je tento postup specifikován zadáním. Ze sekce Role objektů se využije modelu, kdy koncové body jsou původci komunikace. Varianta, kdy se modifikuje průtok dat, nebyla pro tuto práci podstatná, i když by se v praktickém nasazení jistě uplatnila. Typ přenášených dat je **textového charakteru** omezeného na základní ASCII symboly, protože se tím omezuje potřebná bitová délka pro jeden symbol na 8 bitů. V tomto výzkumu bylo uvažováno o úloze steganografie v roli média, kterým dojde k úniku privátního klíče z chráněného síťového perimetru za pomocí **jednosměrného toku dat**. Způsob ochrany však nebyl stanoven, primárním cílem je tedy zjistit vlastnosti steganografického kanálu samotného.

3.2.2 Použité technologie

Povinnou součástí této diplomové práce je i praktická realizace navržených postupů za využití tvorby počítačového programu. Následuje rozpis použitých technologií a platforem, kdy při jejich volbě bylo přihlédnuto ke zkušenostem autora s jejich používáním. Při dalším a detailním rozboru by se jistě daly nalézt vhodnější či lépe optimalizované přístupy, nicméně i současný návrh softwarových komponent je pro řešení vyhovující.

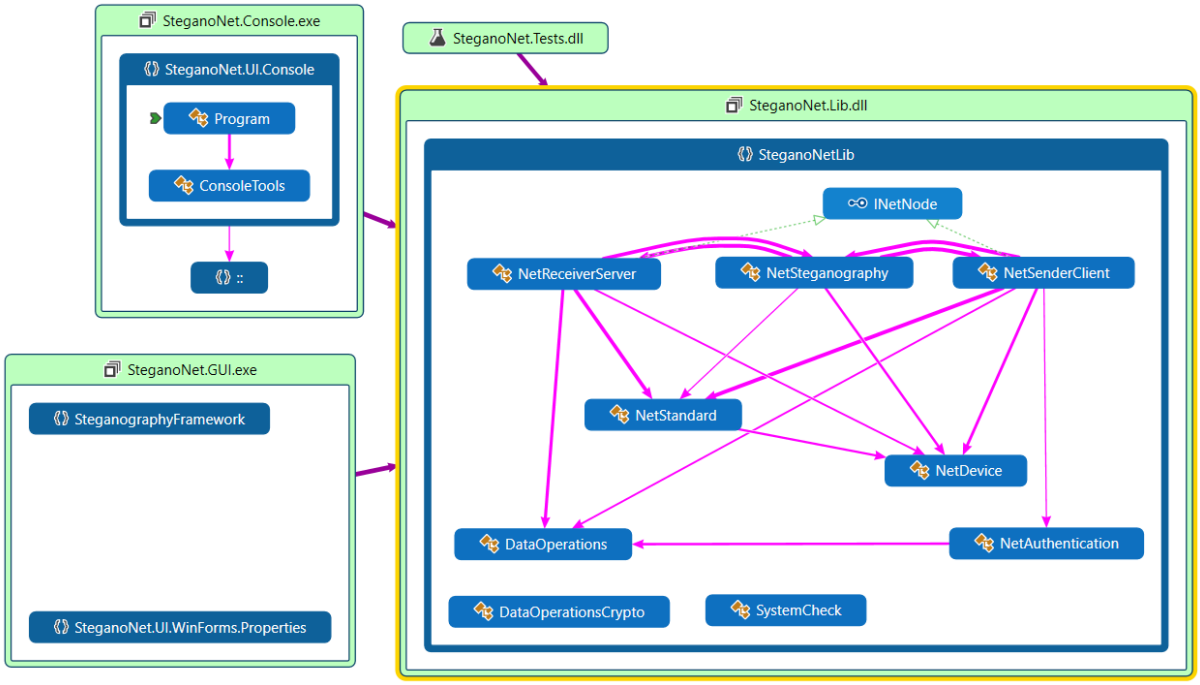
Steganografický síťový framework neboli sada pro testování a snadné rozšiřování skrytého kanálu v prostředí počítačových sítí, je vytvořen pro platformu **Windows**, napsán v jazyce **C#** jako **konzolová aplikace** a s alternativním grafickým rozhraním. Klíčovou pro práci se síťovým provozem TCP/IP je knihovna **PcapDotNet** (nyní ve verzi 0.10.2) z balíčkovacího systému NuGet. Tato volně dostupná mezivrstva zprostředkovává komunikaci vlastního programu a operačního systému. Hlavním benefitem je skutečnost, že je tak možné přistupovat k datagramům objektově a po vrstvách, přičemž lze využívat všechny vlastnosti objektově orientovaného přístupu k programování i při práci s nízko úrovňovými funkcemi síťového rozhraní, které je v rozšířené praxi obvykle doménou programovacích jazyků s nižší abstrakcí (typicky C). Zmíněná knihovna PcapDotNet není jediná svého druhu, existují i podobné variace (například SharpPcap) [33], a ve své podstatě nabízí programátorovi téměř identické služby při obdobných funkcích i výkonu, v obou případech jde o rozhraní k systémovému API WinPcap pro práci se síťovými rozhraními a provozem. Logika pochází z původně linuxové knihovny libpcap, ve které došlo k přenosu funkcionality pro běh na operačním systému Microsoft Windows. Historicky jde o rozšíření síťového ovladače Pcap. V konečném důsledku je tak možné vyvinout počítačový program aplikující steganografii na síťový provoz pro obě hlavní platformy (Windows a Unix). V průběhu evoluce technik programování i systémových volání se přibližuje situace, kdy bude možné stejný program spustit na obou zmíněných platformách bez jejich rozlišení (cross-platform code). K tomuto účelu by mohl být framework .Net Core z dílny Microsoftu, do kterého však není možné v tento moment integrovat knihovnu PcapDotNet, která jej nepodporuje v uvedené verzi. Text práce se dále nezabývá technickým rozlišením hostitelského běhového prostředí a operačního systému.

3.2.3 Architektura aplikace

Program byl v průběhu vývoje rozdělen do vrstev v souladu se správným návrhem softwarového díla. Hlavní artefakt tvoří projekt vytvářející steganografii, který je obsluhován dvěma propojenými projekty s uživatelským rozhraním (konzolovým a grafickým). Jednou z klíčových myšlenek oddělení je zachování principů softwarové knihovny a oddělení referencí na knihovnu PcapDotNet, která není navázaná na uživatelského rozhraní.

Jádrem aplikace je projekt pojmenovaný SteganoNet.Lib, který se dále dělí na třídu serveru-příjemce, klienta-odesilatele, společnou třídu steganografie a množství obslužných tříd a metod rozčleněných podle svého určení. Myšlenkou mezitřídní spolupráce objektů je postup, kdy z vlákna uživatelského rozhraní dojde ke spuštění vlákna serveru nebo klienta podle role konkrétního uzlu. Dané vlákno vytváří a řídí komunikaci s protějškem, přitom volá metody steganografické knihovny, která má společnou bezstavovou implementaci pro obě role odesilatele i příjemce.

Jedním z cílů uvedeného návrhu je umožnit kombinaci více steganografických technik do jednoho datagramu (pokud to dává technicky smysl) a nedojde tím k přepisu jiné ukryté informace. Prakticky se tedy každá z vrstev podle referenčního modelu ISO/OSI vytváří v instanci klienta a podle předchozí volby je dále takový objekt předán na doplnění steganografických informací. V závěru je datagram sestaven a odeslán na server. Na serveru dojde k rozložení na vrstvy a vyčtení ukrytých dat s uložením. Postup pokračuje sémantickou analýzou a přípravou zprávy s odpovědí, která je obratem odeslána klientovi, nebo pokud je protokolem vyžadována. Toto řešení není v jednosměrném skrytém kanálu potřeba, ale dochází tím k ukrývání skutečného významu komunikace a konkrétního datového provozu.

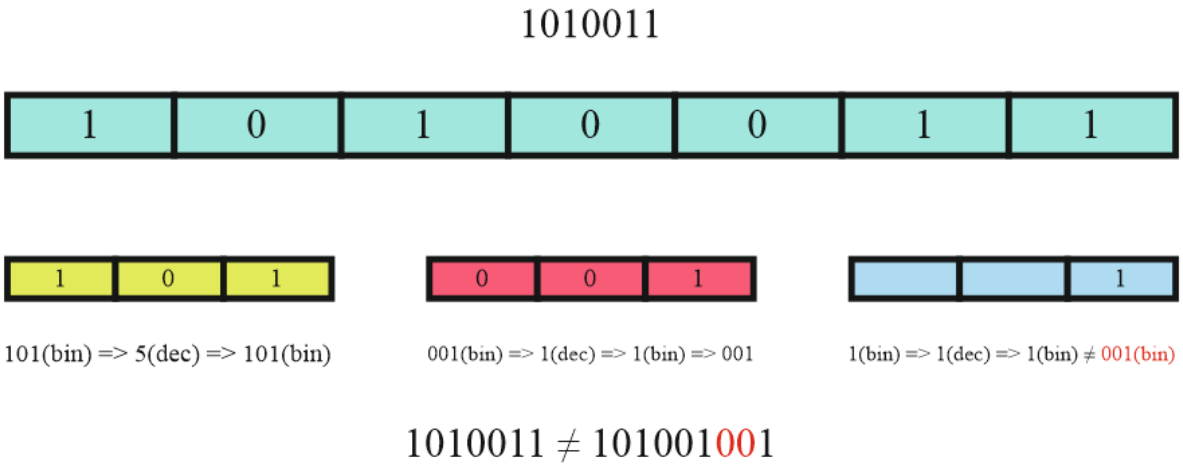


Obrázek 3.4: *Architektura aplikace vizualizovaná nástrojem pro mapování kódu*

Program bylo potřeba doplnit množstvím servisních a podpůrných metod, mezi které patřila také obsluha spojové vrstvy, konkrétně tedy získávání MAC adres, ať už ze zařízení přímo, kde se osvědčilo volat Powershellový skript, protože překvapivě volání systémové knihovny nebylo dostatečně spolehlivé. Mimo jiné bylo potřeba obsluhovat volání ARP protokolu či získat adresu síťové brány, ačkoliv se aplikace přímo zabývá až úrovněmi nad touto. Z funkcionality vyšších vrstev bylo vyčítáno doplňkovou metodou například i místní úložiště doménových dotazů, jelikož se tyto hodnoty využívají pro krycí dotazy obsahující steganografii.

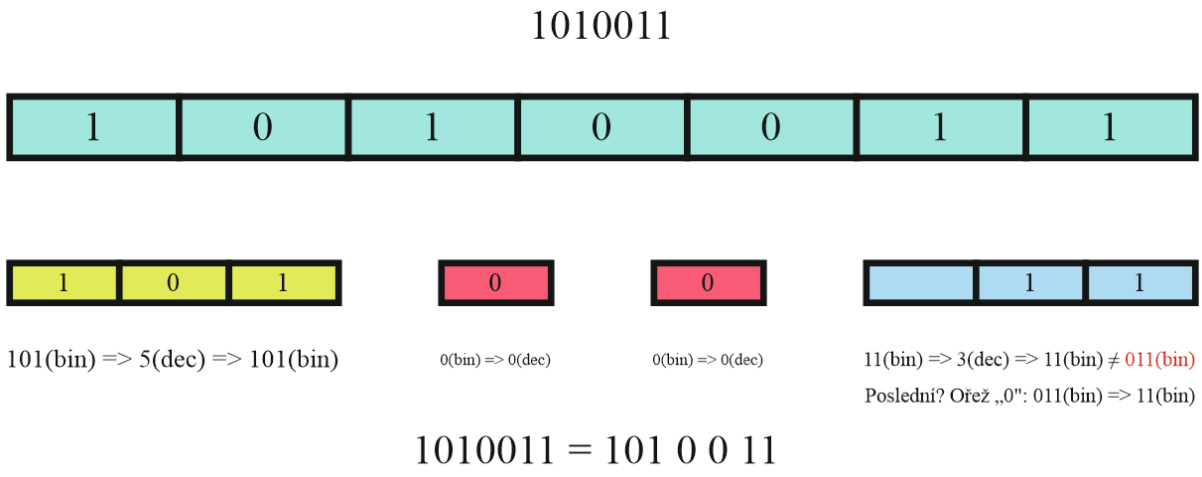
Komunikaci se síťovým rozhraním zajišťuje otevření adaptéru a zahájení odchytávání procházejících paketů tak, jak jej známe ze softwarových analyzátorů provozu. Zásadním pro zpracování výsledků je správné vytvoření filtrů, protože zejména na jediném síťovém připojení počítače je značný provoz, který se steganografickou komunikací nesouvisí. Dobře nastavený filtr výrazným způsobem ovlivňuje výkonnost programu a snižuje počet falešně označených zpráv pro zpracování.

Dosud se v textu hovořilo o technickém prostoru k ukládaní vlastních dat, nicméně samotná steganografická zpráva má také svůj formát. Zadání vycházelo z předpokladu přenosu textového řetězce tvořeného ASCII symboly. Pro přenos v jednotlivých bitech hlaviček se nabízelo převést jej do binární podoby řetězce jedniček a nul, poté vyčítat je přímo z konkrétních bitů hlaviček. Zásadní komplikací implementace byla skutečnost, že data jsou převáděna do decimální podoby při práci s knihovnou PcapDotNet, čímž docházelo k ořezu úvodních nul řetězců, které musely být doplňovány zarovnáním do původní délky. Teoretický model tak narazil v praxi na skutečnost problematického určování délky řetězce s utajenou zprávou, což nevadilo v průběhu přenosu, ale zásadně se to projevovalo v posledním bloku přenášené zprávy (který nevyužívá plnou délku daného pole hlavičky).



Obrázek 3.5: *Znázornění problému přenosu binárního řetězce neznámé délky*

Řešením první zmíněné komplikace je podmínka, která zakazuje posílat řetězec obsahující nulu na začátku, ta musí být odeslána samostatně. Přijímací strana tak do svého bloku zapíše pouze jeden nulový znak nezávisle na počtu nul přijatých. Tento postup však nevyřeší problém posledního bloku, kde chybí bity k přenosu, a jsou tak doplněny nuly. Při zpracování přijaté zprávy jsou všechny úvodní nuly u řetězců delší jedné ořezány.



Obrázek 3.6: *Znázornění řešení problému přenosu binárního řetězce neznámé délky*

Použitý a zde popsaný postup vytváří problém v některých hlavičkách, jelikož přenos nuly je viditelně podezřelý a je třeba jej zvlášť maskovat. Souvisejícím problémem je skutečnost, že zvyšuje počet přenášených zpráv, zejména u metod využívajících pouze několik bitů. Neefektivita takového postupu je daná formou přenosu a požadavku na libovolnou délku zprávy, respektive možností, že blok nevyužije celou délku svého pole. V případě, že by bylo rozdělení zprávy na bloky beze zbytku, by nebyl tento postup potřeba. Nicméně v této implementaci je možnost kombinovat několik umístění steganografie v datagramu současně, kdy se mění dělitelé a to i do kombinací, kdy největší společný dělitel neúměrně prodlužuje zprávu, což není žádoucí. V porovnání s tím je použitý přenos několika nulových zpráv méně nákladný.

Shrnutí: Ke snadnějšímu postupu implementace by pomohla některá omezující podmínka na délku řetězce v bitech, který je beze zbytku dělitelný bitovou kapacitou, čímž by odpadla starost o zarovnání. Nevýhodou v tomto směru je pak poměrně výrazné omezení uživatele nebo nutnost implementace dalších podpůrných, avšak komplexnost navyšujících, metod. Jako další řešení se nabízí výměna informace o délce přenášené zprávy v části sestavující spojení. Při rekonstrukci řetězce by tak bylo známo, jestli má být blok zarovnán či nikoliv.

Jako vhodné se ukazuje nepřevádět data do binárního tvaru, ale převést vstupní textový řetězec do jiné podoby, například jeho ponecháním v decimálních hodnotách ASCII znaků a přenosu v číslicích. Zde taktéž záleží, zdali by bylo možné vstupní data bezztrátově převést do decimálního formátu.

Přenos řetězce otevírá otázku, jak v cíli **ověřit, že přenos proběhl bez chyby**. Zde je vhodné využít některé z metod detekcí a opravy chyb uvedených v sekci Robustnost. Konkrétně pak bylo využito MD5 hashe z přenášené zprávy v ASCII, která je připojena za vlastní zprávu, a poté společně převedena do (binárního) formátu kanálu. Délka tohoto hashe není variabilní, ale jde o pevně nastavený blok specifikované délky, na který je výsledek funkce MD5 ořezán, čímž může docházet ke kolizím unikátnosti. Při testování se ukázalo, že při vhodně nastaveném poměru délky hashe a původního řetězce jsou kolize marginální a schopnost rozpoznat poškozený řetězec je téměř jistá.

Rozpoznání protistrany a její ověření bylo navrženo s použitím CHAP přístupu popsaného v sekci Sestavení spojení. Teoreticky jde o předřazenou metodu, která za si pomocí některé z obousměrných metod (typicky odpověď na dotaz) a ideálně z množiny zvolených technik vymění sdílené tajemství. Jelikož prakticky tento přístup vyžaduje implementaci příslušných metod, byla ze začátku použita metoda statického omezení provozu pomocí filtrů na rozhraní Pcap, jehož inicializační hodnoty byly převzaty z uživatelského nastavení. Prakticky tak docházelo k omezení zdrojové IP adresy, portu a protokolu k rozpoznání spojení. I toto řešení je v mnoha případech dostačující, jeho výhodou je nižší počet zpráv nutných k zahájení přenosu. Hlavním omezením je však nutnost znát provozní síťové hodnoty na druhé straně uzlu, což v praxi vyžaduje předání této informace postranním kanálem, který nemusí být dostupný. Druhou komplikací je skutečnost, že se některé z nastavených adres mohou dynamicky v průběhu přenosu změnit (například při průchodu uzlem s překladem adres či portů) a takto realizované sestavení spojení poté není funkční, protože neočekává jiné příchozí hodnoty.

3.2.4 Praktická omezení

V průběhu testování byla identifikovány limity a některé nepředpokládané skutečnosti řešení. Jedním ze známých omezení je potřeba instalace zmíněné knihovny WinPcap pro zachycení a odesílání modifikovaného síťového provozu, která potřebuje administrátorská oprávnění hostitelského systému. Tato práce má akademický charakter, a tak při legitimním užití nejde o komplikaci. Dále je potřeba, aby byl server (příjemce komunikace) přístupný ze sítě, zejména vstupuje-li do trasy překlad adres (NAT), což je potřeba si uvědomit při inicializaci spojení nebo provést přesměrování portů. V implementaci, která používá sestavení spojení na základě statických hodnot, je pak u některých metod nepřekonatelným problémem překlad adres, avšak zásadnější omezení vytváří překlad portů (PAT), který způsobí, že server neodpoví na příchozí požadavek na jiném než očekávaném portu. Marginálním, avšak testování omezující skutečností, se stal problém, kdy některé ovladače zejména virtuálních síťových karet v lokálních hostitelích i v testovaném cloudovém prostředí Azure neotevíraly svá rozhraní a program končil výjimkou, jejíž příčinu se nepodařilo ve vyhrazeném čase odhalit. Jak se také ukázalo, pokud je rozhraní, na kterém program běží nestabilní, dojde při jeho výpadku k výjimce a přerušení činnosti.

4 Měření skrytého kanálu

4.1 Použité metody

Pro testování reakcí různých síťových prostředí byly vybrány některé z implementovaných metod. Protože program byl navrhnut pro možnost kombinování více různých steganografických míst, jsou zkoušeny nejen samostatné metody, ale také jejich kombinace.

Zpracování programem vyžaduje použití identifikátorů (hodnota ID metody), které byly navrženy bez další návaznosti (jsou jen lokálně signifikantní), i když si ponechávají jistou logiku odkazující na referenční model TCP/IP v první číslici. Druhá číslice rozděluje bloky podobných metod v rámci stejné vrstvy. Poslední číslice označuje konkrétní metody, přičemž sudá hodnota je ponechána pro případnou lehkou vývojovou modifikaci její liché varianty. Rezervována byla číslice nula v posledním řádu pro označení skupiny metod podobně, jako se děje u subnetů IP adres. Interní prioritou při souběžném umisťování skrytých dat je hodnota ID se vzestupnou orientací, respektive vybírání pracuje v režimu fronty.

Tabulka 4.1: *Přehled zkoušených metod*

ID	Protokol	Hlavička	Prostor [b]
301	IP	DiffServ	8
303	IP	Identification	16
305**	IP	MF offset	13*
333	ICMP	Echo Identifier	16
335	ICMP	Echo Sequence	16
703	DNS	Transaction ID	16
705	DNS	Response IP	32
733	HTTP	GET URL	64

**metoda, jejíž kapacita přenosu není konstantní*

***metoda, kterou nelze použít samostatně*

Tabulka 4.2: *Přehled zkoušených kombinovaných metod*

ID	Hlavní protokol	Prostor [b]
301, 303, 305, 333, 335	ICMP	69*
303, 305, 333, 335	ICMP	61*
303, 333, 335	ICMP	48
333, 335	ICMP	32
703, 705	DNS	48
301, 705	DNS	40
303, 705	DNS	48

**metoda, jejíž kapacita přenosu není konstantní*

U některých metod není jisté, že jejich prostor bude využit, protože pro aplikaci steganografie do jejich hlaviček existují technická omezení, jejichž vlastnosti je nedovolují využít pokaždé. IP identification se mění po určitém časovém intervalu (IETF doporučuje 2 minuty), v následujících měření je přenastaveno na 10 sekund (viz tabulka 4.3), kdy dochází k výměně náhodné hodnoty za úmyslně změněnou. U metody využívající příznak MF a pole offset je podmínka, že hodnota offsetu musí být beze zbytku dělitelná 8 (protože jde o ukazatel), pokud tato podmínka není naplněna, příznak není nastaven, a ani protější strana toto pole dále nezpracovává. Hodnoty dalších časovačů vycházely z RFC, v průběhu vývoje byly nastaveny na následující zejména z důvodu udržení rozumné propustnosti kanálu v průběhu testování. Předpokládá se, že jejich hodnota může být změněna v závislosti na konkrétním prostředí opět na hodnoty dané standardem i za cenu výrazné snížení propustnosti kanálu.

Tabulka 4.3: *Přehled použitých časovačů při odesílání zprávy*

Protokol	Popis	Hodnota [ms]	Hodnota RFC [ms]
Všechny	obecná prodleva mezi vysíláním	500	
IP	změna pole identifikace	10 000	120 000
ICMP	čas mezi vysíláním požadavků	1 000	
TCP	čekání na odpověď	10 000	120 000
DNS	čas vyčkávání na odpověď	3 000	

V průběhu testování bylo potřeba rovněž pracovat s časovými hodnotami mezi jednotlivými odeslanými zprávami. Nastavení časovačů má zásadní vliv na kapacitu kanálu, ale také na riziko odhalení. Prakticky je možné odeslat celou tajnou zprávu téměř v jeden moment, avšak takový přístup většinou porušuje princip fungování hostitelského protokolu, čímž na sebe upozorňuje. RFC definuje některé z těchto časovačů, další jsou definovány operačním systémem. V průběhu testování byly použity výše uvedené hodnoty, které vycházely z pozorování standardního provozu, či byly odladěny k uspokojivým parametrům přenosu. Jejich hodnotu lze změnit, a dosáhnout tak jiných výsledků.

4.2 Testovací zpráva

Pro zkušební provoz byly vybrány k přenosu dvě textové zprávy zastupující řetězec privátního klíče, pro snadnější rozpoznání byly použity lidsky přívětivé věty. Formátování a dostupná znaková sada vychází ze symbolů ASCII a jejich numerických rozsahů, kdy lze uvažovat 8 bitů pro znak. Podpora rozšířených znakových sad není teoretický problém, je však potřeba zvážit jejich vliv na délku binárního řetězce, do kterého jsou znaky převáděny. V případě nutnosti podpory mezinárodních znaků a češtiny by stálo za reimplementaci formátu kanálu do dekadického či hexadecimálního formátu, nebo lépe převedení do kódování base-64, které konvertuje binární řetězce na text, pak je ale potřeba signalizovat protistraně, že data jsou v tomto formátu.

Restrikce vstupu na ASCII symboly zvýhodňuje například použití angličtiny jako přenosového jazyka, případně se také hodí pro transport kryptografických klíčů. V ideálním případě by mělo dojít také k zašifrování řetězce pro minimalizaci opětovného sestavení komunikace a získání zprávy. V implementaci programu bylo s tímto požadavkem počítáno, avšak z důvodu izolace výzkumu steganografie vrací kryptografické funkce text v identické podobě jako na jejich vstupu.

Zpráva A: počet znaků textu 43, délka zprávy v binární podobě: 344 znaků, ověřovací hash: 9e107d9d372bb6826bd81d3542a419d6, hash po ořezání na délku 16 znaků 9e107d9d372bb682 v 128 znacích binárního řetězce, celková délka: 472 bitů, zpráva:

```
The quick brown fox jumps over the lazy dog
```

Zpráva B: počet znaků textu 107, délka zprávy v binární podobě: 1688 znaků, ověřovací hash: 3d4bc48402778bc367fd4d727f4366ec, hash po ořezání na délku 16 znaků 3d4bc48402778bc3 v 128 znacích binárního řetězce, celková délka: 1816 bitů, zpráva:

```
VSB - Technical University of Ostrava has long tradition in high
quality engineering. Our study programmes stand on a tradition going
back more than 165 years, but reflect current, state of the art
technologies.
```

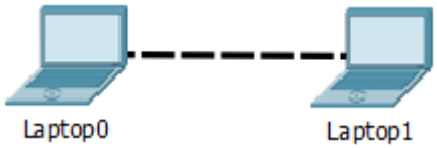
4.3 Testování v různých prostředích

Pro ověření funkčnosti byl vytvořen powershellový skript volající konzolovou aplikaci s parametry potřebnými pro dané testování v cyklech pro jednotlivé metody a testovací zprávy. Tato konfigurace umožnila eliminaci chyb danou konfigurací a částečnou automatizaci. Pro ověření spojení mezi dotčenými uzly byl proveden kontrolní ping či obdobný krok před zahájením komunikace.

- při měření jsou uváděny identifikátory měření, podle nichž je možné najít záznam testu v souborech přílohy.
- měření se odehrávalo geograficky ve Finsku

4.3.1 Přímé Ethernetové spojení

Jedním ze základních scénářů je funkčnost na nejkratší možnou vzdálenost. Dva fyzické počítače byly spojeny kříženým ethernetovým kabelem a síťové nastavení bylo provedeno statickými IP adresami. Toto zapojení má výhodu, že do něj nevstupuje žádný další prvek, který by ovlivnil nějaké z hlaviček protokolů.



Obrázek 4.1: *Schéma topologie při testování přímého spojení počítačů*

Prakticky je prostředí přímo spojených počítačů pro aplikaci steganografie bezúčelné, slouží však k ověření funkčnosti řešení v průběhu vývoje. Nevýhodou je nutnost dvou fyzických zařízení.

Pro potřebu testování při vývoji nezávisle na okolním síťovém prostředí bylo používáno otevření **komunikace na rozhraní localhost** (zpětné smyčky), případně jednoho z přítomných fyzických síťových adaptérů. Tím odpadla potřeba dvou počítačů, situaci však zkomplikovala skutečnost, že v takto uspořádané topologii je rozhraní odesílatele a příjemce totožné. Nastane tak situace, kdy je obtížné od sebe odlišit datagramy odchozí a příchozí a je potřeba rovněž změnit filtry provozu. Orientace v zachyceném provozu je vinou totožných identifikátorů obou stran obtížná. Pro potřeby vývoje s omezenou možností testování je však toto řešení použitelné.

Obrázek 4.2: *Schéma topologie při testování na rozhraní zpětné smyčky*

Tabulka 4.4: *Tabulka výsledků měření na rozhraní zpětné smyčky pro zprávu A*

			zpráva A			
Číslo testu	**ID metody**	**Prostor [b]**	**Počet zpráv**	**Čas [s]**	**Čas [ms]**	**Úspěch**
431.01-A	301	8	61	60	60 535	ano
431.02-A	303	16	311	311	311 857	ano
431.03-A	333	16	32	31	31 344	ano
431.04-A	335	16	32	31	31 439	ano
431.05-A	703	16	32	94	94 151	ano
431.06-A	705	32	17	50	50 078	ano
431.07-A	733	64	11	76	76 919	ano
431.08-A	301, 303, 305, 333, 335	69	14	13	13 305	ano
431.09-A	303, 305, 333, 335	61	19	18	18 304	ano
431.10-A	303, 333, 335	48	15	14	14 280	ano
431.11-A	333, 335	32	16	15	15 305	ano
431.12-A	703, 705	48	11	31	31 504	ano
431.13-A	301, 705	40	13	37	37 320	ano
431.14-A	303, 705	48	15	43	43 677	ano

Tabulka 4.5: *Tabulka výsledků měření na rozhraní zpětné smyčky pro zprávu B*

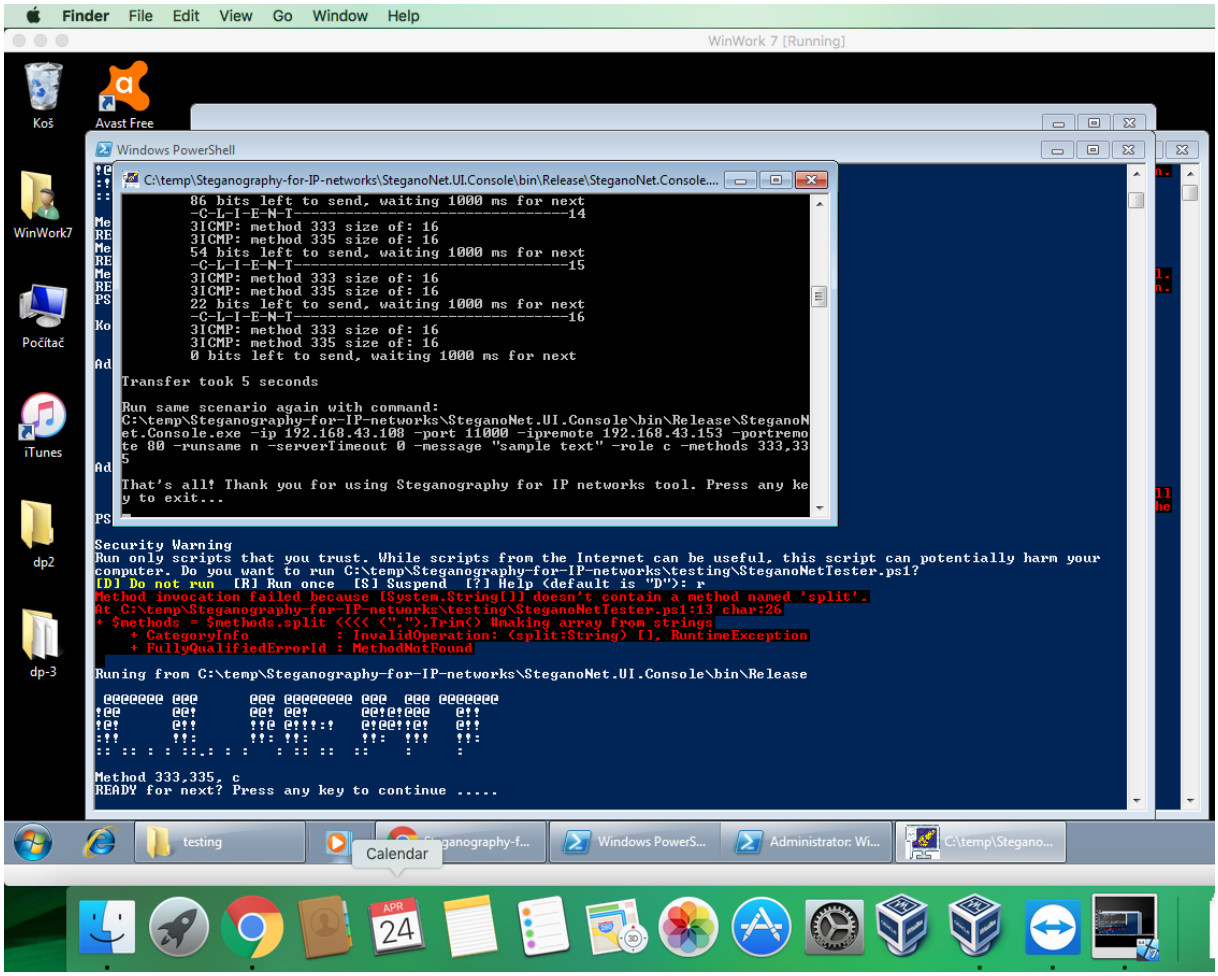
			zpráva B

Číslo testu	ID metody	Prostor [b]	Počet zpráv	Čas [s]	Čas [ms]	Úspěch
431.01-B	301	8	256	256	256 124	ano
431.02-B	303	16	1221	1227	1 227 822	ano
431.03-B	333	16	123	122	122 523	ano
431.04-B	335	16	123	123	123 184	ano
431.05-B	703	16	123	368	368 316	ano
431.06-B	705	32	67	200	200 039	ano
431.07-B	733	64	32	229	229 778	ano
431.08-B	301, 303, 305, 333, 335	69	57	56	56 430	ano
431.09-B	303, 305, 333, 335	61	69	68	68 437	ano
431.10-B	303, 333, 335	48	59	58	58 632	ano
431.11-B	333, 335	32	62	61	61 432	ano
431.12-B	703, 705	48	43	127	127 935	ano
431.13-B	301, 705	40	46	136	136 910	ano
431.14-B	303, 705	48	58	172	172 746	ano

Z výsledků vyplývá, že počet zpráv odpovídá celkové bitové délce přenášeného řetězce děleno kapacitou dané metody. Zprávy nad rámec tohoto výpočtu odpovídají nutnosti přenášet nuly na začátku řetězců samostatně. Podrobnější analýza je obsažena v kapitole Parametry skrytého kanálu. Čas přenášení odpovídá počtu zpráv a nastavenými prodlevami mezi nimi (viz tabulka 4.3). V tomto případě se výsledky shodují s očekáváními, rychlost a spolehlivost přenosu je díky běhu na jednom počítači bez negativního vlivu přenosové trasy a hodnoty lze použít jako referenční.

Poslední variantou možného lokálního testování byla **vnitřní síť virtuálního stroje**. Software pro hostování virtuálních počítačů umožňuje základní konfiguraci přístupu běžících instancí k síti, k čemuž používá rozhraní v hostitelském operačním systému, na kterých je možné spustit zachytávání. Odpadá tak problém zmíněný výše při testování na rozhraní localhost, protože jsou adaptéry fyzického operačního systému a virtuálního operačního systému navzájem odlišné. Hodnoty při měření zejména rychlosti se odlišovaly pouze marginálně od výsledků při testování na zpětné smyčce, a proto nejsou samostatně uvedeny.

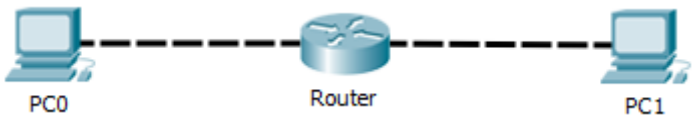
V kapitole Praktická omezení byla zmíněno, že aplikace se nemusí rozběhnout při používání rozhraní virtuálního stroje. Z neznámých příčin se takové chování neprojevilo při použití software VirtualBox. Podstatou virtualizace je oddělení operačních systémů, díky které se podařilo rozběhnout steganografickou aplikaci i na počítači Apple Mac s Apple OS, a díky přemostěnému přístupu k síti v nastavení VirtualBoxu tak datagramy působily na straně příjemce jako skutečně nativně odeslané z tohoto zařízení. Tímto postupem by bylo možné využít běhu z hostitelských operačních systémů Linux a podobných. Zjednodušeným modelem nevyžadující nasazení plné virtualizace by pak mohlo být užití některých z kontejnerovacích služeb typu Docker, což už však nebylo prakticky ověřováno.



Obrázek 4.3: *Snímek obrazovky zachycující běh virtuálního stroje a instance aplikace*

4.3.2 Lokální síť pevná

Jedním ze základních scénářů pro testování se skutečným fyzickým přenosem je test v lokální síti LAN po metalickém vedení technologií Ethernet přes síťový prvek přepínač, respektive byl použit router, avšak při komunikaci v rámci stejného IP subnetu je provoz přepínán a nikoliv směrován. Při implementaci vyplynulo, že v tomto scénáři není nutné vyplňovat korektně hlavičku spojové (druhé) vrstvy referenčního modelu ISO/OSI, konkrétně obě MAC adresy, protože i přes inicializaci nulovými adresami je zpráva doručena příjemci. Přepínač se dotáže na konkrétního příjemce pomocí ARP dotazu vytvořeného z IP adresy a následně doručí rámec správnému uzlu.

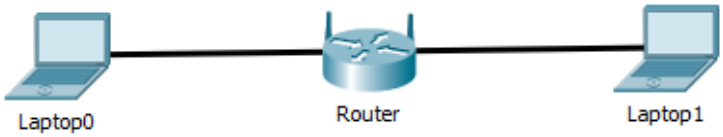


Obrázek 4.4: *Schéma topologie při testování v lokální metalické síti Ethernet*

Výsledky měření v této síti nejsou publikovány ve zvláštní tabulce, protože se téměř nelišily od hodnot získaných v sítích bezdrátových v následující kapitole.

4.3.3 Lokální síť bezdrátová

Pro testování byly použity dva fyzické notebooky na platformě Windows v stejném síťovém subnetu připojené protokolem 802.11ac v pásmu 5 GHz přes Cisco AP. Kritické pro testování spojení přes WiFi je správné uvedení fyzických (MAC) adres v hlavičkách.



Obrázek 4.5: *Schéma topologie při testování v lokální bezdrátové síti WiFi*

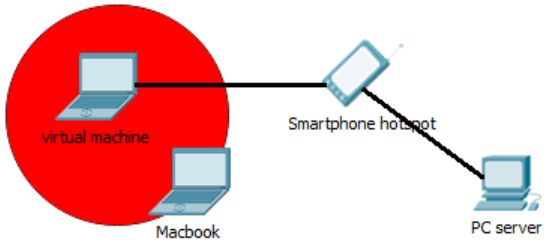
Tabulka 4.6: *Výsledky měření při použití WiFi v lokální síti*

			zpráva A		
Číslo testu	**ID metody**	**Prostor [b]**	**Počet zpráv**	**Čas [s]**	**Úspěch**
433.01	301	8	61	60	ano
433.02	303	16	311	310	ano
433.03	333	16	32	31	ano
433.04	335	16	32	31	ano
433.05	703	16	32	95	ano
433.06	705	32	17	50	ano
433.07	733	64	11	92	ano
433.08	301, 303, 305, 333, 335	69	14	13	ano
433.09	703, 705	48	11	32	ano
433.10	301, 705	40	13	38	ano
433.11	301, 733*	72	8	88	ne

**Úspěchu v tomto případě nebylo dosaženo u kombinace metody 301 (IP DiffServ) a 733 (HTTP GET) z důvodu, že protokol HTTP navazuje spojení pomocí protokolu TCP, který rovněž využívá hlaviček IP. Program v dané verzi správně nerozeznává, které datagramy steganogram obsahují, proto metoda selhává ve schopnosti zprávu rozpoznat.*

Výsledky v tomto měření opět nepřekvapují, hodnoty odpovídají očekáváním. Je možné konstatovat, že vliv fyzického přenosového média a standardů IEEE 802.11 (WiFi) či 802.3 (Ethernet) je zanedbatelný, tyto technologie jsou pro komunikaci v rádiově nezarušeném prostředí plně srovnatelné.

V rámci testování zařízení bylo taktéž ověřena schopnost předávání zpráv mobilním hotspotem. Pokus je zařazen zde, neboť šlo o lokální bezdrátovou síť, ačkoliv ji netvořil žádný dedikovaný síťový prvek. Ze zkušeností vyplývá, že toto řešení by trpělo nedostatkem propustnosti až ve chvíli velkého zatížení mnoha klienty. Byl zde taky prakticky vyzkoušen případ, kdy virtuální počítač s OS Windows používá síťovou kartu svého hostitele s Mac OS.



Obrázek 4.6: *Schéma topologie při testování v lokální bezdrátové síti v netypickém provedení*

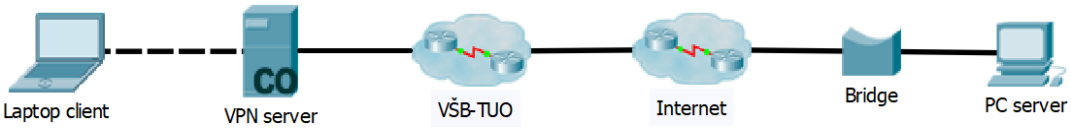
Tabulka 4.7: *Tabulka vybraných měření při použití lokální sítě tvořené Android hotspotem*

			zpráva A		
Číslo testu	**ID metody**	**Prostor [b]**	**Počet zpráv**	**Čas [s]**	**Úspěch**
433.07.2	733	64	11	12	ano
433.09.2	703, 705	48	11	34	ano
433.12.2	333, 335	32	16	16	ano

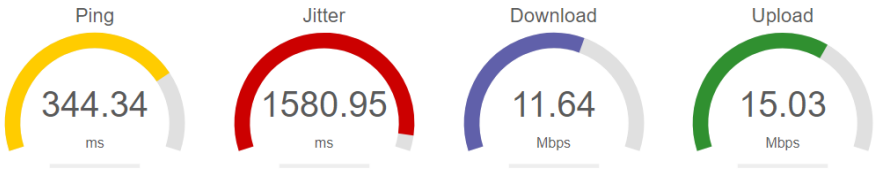
4.3.4 Internet

Průchod sítí Internet byl ověřován dvěma způsoby, jednak z akademické sítě VŠB-TUO po připojení k VPN koncentrátoru. V tomto prostředí je známo, že správci dbají na bezpečnostní rizika a lze očekávat jistý stupeň ochrany na rozhraní univerzitní sítě a Internetu. V druhém případě pak byla použita veřejná WiFi síť pro návštěvníky finského města Jyväskylä.

4.3.4.1 Akademická síť



Obrázek 4.7: *Schéma topologie sítě při testu průchodností Internetem s použitím VPN. Mezi laptopem a VPN koncentrátorem je navázán IPSec tunnel*



Obrázek 4.8: *Parametry sítě při připojení VPN do akademické sítě VŠB*

```
C:\Users\ivo>tracert 84.251.160.115

Tracing route to dsl-jklbng12-54fba0-115.dhcp.inet.fi [84.251.160.115]
over a maximum of 30 hops:

  1   130 ms    60 ms    59 ms  158.196.99.33
  2     *         *       59 ms  158.196.99.73
  3     *         *        *     Request timed out.
  4     *         *        *     Request timed out.
  5     *         *        *     Request timed out.
  6     *         *        *     Request timed out.
  7     *         *        *     Request timed out.
  8     *         *        *     Request timed out.
  9     *         *        *     Request timed out.
 10     *         *        *     Request timed out.
 11     *         *        *     Request timed out.
 12     *         *        *     Request timed out.
 13   109 ms   108 ms   108 ms  dsl-jklbng12-54fba0-115.dhcp.inet.fi [84.251.160.115]

Trace complete.
```

Obrázek 4.9: *Záznam trasy mezi klientem a serverem v akademické síti*

Tabulka 4.8: *Výsledky měření skrytého kanálu při průchodu Internetem ze sítě VŠB pro zprávu A*

			zpráva A		
Číslo testu	**ID metody**	**Prostor [b]**	**Počet zpráv**	**Čas [s]**	**Úspěch**
434.01.1-A	301	8	61*	60	ne
434.02.1-A	303	16	311*	311	ne°
434.03.1-A	333	16	32*	31	ne°
434.04.1-A	335	16	32*	31	ne°
434.05.1-A	703	16	32	94	ano**
434.06.1-A	705	32	17	49	ano**
434.07.1-A	733	64	x	x	ne°
434.08.1-A	301, 303, 305, 333, 335	69	12	11	ne
434.09.1-A	303, 305, 333, 335	61	19	18	ne°
434.10.1-A	303, 333, 335	48	15	14	ano
434.11.1-A	333, 335	32	16	15	ano
434.12.1-A	703, 705	48	11	31	ano**
434.13.1-A	301, 705	40	13	37	ne**
434.14.1-A	303, 705	48	15	43	ano**

**spojení bylo přerušeno mezi serverem a klientem*

*** na nestandardním portu, na standardním „ne“*

° *neočekávaný výsledek*

x – nebylo navázáno spojení

Tabulka 4.9: *Výsledky měření skrytého kanálu při průchodu Internetem ze sítě VŠB pro zprávu B*

			zpráva B		
Číslo testu	ID metody	Prostor [b]	Počet zpráv	Čas [s]	Úspěch
434.01.1-B	301	8	x	x	x
434.02.1-B	303	16	x	x	x
434.03.1-B	333	16	x	x	x
434.04.1-B	335	16	x	x	x
434.05.1-B	703	16	123	367	ano**
434.06.1-B	705	32	67	199	ano**
434.07.1-B	733	64	x	x	x
434.08.1-B	301, 303, 305, 333, 335	69	x	x	x
434.09.1-B	303, 305, 333, 335	61	x	x	x
434.10.1-B	303, 333, 335	48	59	58	ne°
434.11.1-B	333, 335	32	62	61	ne°
434.12.1-B	703, 705	48	43	127	ano**
434.13.1-B	301, 705	40	46	136	ne**
434.14.1-B	303, 705	48	58	172	ne**°

x – nebylo čekáno na dokončení odesílání z důvodu, že je přenos zřejmě poškozen

*** na nestandardním portu, na standardním „ne“*

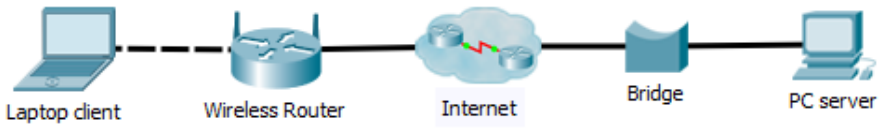
° *neočekávaný výsledek*

U měření v sítí VŠB se projevil vliv nějaké z ochran typu IPS, kdy byl generovaný provoz po přibližně 30 zprávách protokolu ICMP zablokován, standardní ICMP echo požadavky nebyly tímto zasaženy. Pokud měla zpráva méně částí, mechanismus pro blokování zřejmě nestihnul hrozbu vyhodnotit a zablokovat. Toto chování bylo vysledováno z jiného počtu přijatých a odeslaných zpráv. Dle očekávaní došlo ke ztrátě informace uložené v poli DiffServ metody 301 (podrobněji rozvedeno v kapitole Spolehlivost), taktéž pakety obsahující fragmentaci byly ztraceny, což bylo očekáváno.

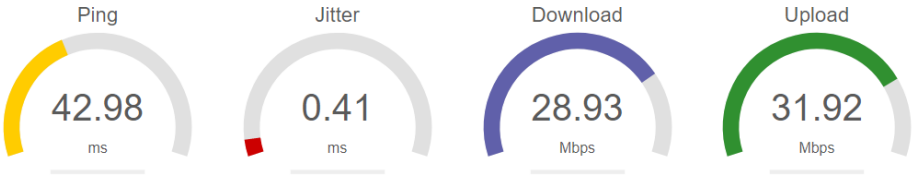
Je rovněž známo, že správci univerzitní sítě VŠB blokují z bezpečnostních důvodů provoz na jiné než univerzitní DNS servery, proto komunikace na standardním portu 53 nebyla navázána, avšak spojení bylo úspěšné na jiném portu z dynamického rozsahu. Je nutné se zamyslet, zdali je DNS komunikace na nestandardním portu stále vhodným kanálem ke steganografii. Z neznámých příčin pak nebyla klientem přijata odpověď na TCP SYN požadavek, který server odeslal zpět, a proto nedošlo k sestavení spojení u metody 733 používající HTTP, kdy v cestě nedošlo k překladu portů.

Taktéž se v tomto měření plně projevila absence mechanismu zajišťující spolehlivost, protože zejména u bitově delší a na počet datagramů delší zpráva B nebyla opětovně sestavena vlivem poškození při přenosu, ačkoliv přenos zprávy A v tomtéž prostředí fungoval. Akademická síť VŠB-TUO byla také množstvím síťových omezení nejvíce střeženým prostředním v tomto testu.

4.3.4.2 Městská veřejná WiFi síť



Obrázek 4.10: *Schéma topologie sítě při testu průchodností Internetem z veřejné WiFi sítě*



Obrázek 4.11: *Parametry sítě při připojení na městskou WiFi síť*

```
C:\Users\ivo>tracert 84.251.160.115

Tracing route to dsl-jklbng12-54fba0-115.dhcp.inet.fi [84.251.160.115]
over a maximum of 30 hops:

  1    21 ms     1 ms     1 ms  10.203.0.1
  2     2 ms     2 ms     1 ms  172.20.89.141
  3     5 ms     5 ms     5 ms  xe3-2-0-4.helpa-gw1.fi.elisa.net [139.97.7.25]
  4     5 ms     5 ms     6 ms  sonera-gw.1.fi.elisa.net [139.97.7.26]
  5     9 ms     9 ms     9 ms  141.208.192.18
  6     9 ms     9 ms     9 ms  dsl-jklbng12-54fba0-115.dhcp.inet.fi [84.251.160.115]

Trace complete.
```

Obrázek 4.12: *Záznam trasy mezi klientem a serverem*

Tabulka 4.10: *Výsledky měření steganografického kanálu při průchodu Internetem*

			zpráva A		
Číslo testu	**ID metody**	**Prostor [b]**	**Počet zpráv**	**Čas [s]**	**Úspěch**
434.01.2	301	8	61	60	ne
434.02.2	303	16	311	314	ano
434.03.2	333	16	32	31	ne°
434.04.2	335	16	32	31	ano
434.05.2	703	16	32	94	ne°
434.06.2	705	32	17	49	ne°
434.07.2	733	64	x	x	ne
434.08.2	301, 303, 305, 333, 335	69	14	13	ne
434.09.2	303, 305, 333, 335	61	19	18	ne°
434.10.2	303, 333, 335	48	15	14	ano
434.11.2	333, 335	32	16	15	ne°
434.12.2	703, 705	48	11	31	ne°
434.13.2	301, 705	40	13	37	ne
434.14.2	303, 705	48	15	43	ne°

x – nebylo čekáno na dokončení odesílání z důvodu, že je přenos zřejmě poškozen

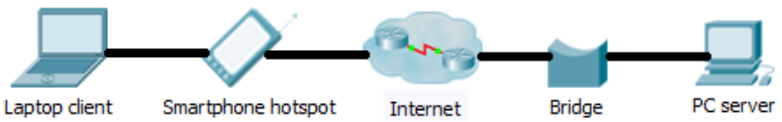
° *neočekávaný výsledek*

Měření v této sítí ukázala, že aktuálně navržený kanál je náchylný na ztrátu paketů způsobenou přenosem. Úroveň signálu bodu byla v tomto měření nejnižší z důvodu vyšší fyzické vzdálenosti k přístupovému bodu. Tento rozdíl pak ukazuje, že ve 14 pokusech bylo 9 případů s výskytem ztráty, 3 úspěšné přenosy a 2 případy ostatní. Měření ukázalo, že v praktickém použití s hůře dostupnou sítí by bylo potřeba zapracovat na mechanismu kontroly spolehlivosti.

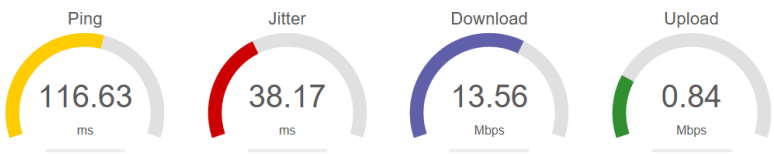
Překvapením jsou numericky neočekávané naměřené časy přenosů, kdy místní sítě mají v podstatě tytéž délky trvání vysílání a příjmu jako přenos přes síť Internetu (respektive rozdíly byly na úrovni chyby měření). Prakticky se ukazuje, že kvalitní přístupové sítě stírají rozdíl mezi lokálními a vzdálenými síťovými zdroji při použití běžného IT vybavení.

4.3.5 Internet mobilní

Pro test byl použit mobilní telefon se systémem Android připojený pomocí konektivity 4G+ do sítě finského operátora Saunalahti (Elisa).



Obrázek 4.13: *Schéma topologie při testování v buňkové síti*



Obrázek 4.14: *Parametry připojení k Internetu v buňkové síti (PC na hotspotu)*

```
C:\Users\iiris>tracert 84.251.221.209

Tracing route to dsl-jklbng12-54fbdd-209.dhcp.inet.fi [84.251.221.209]
over a maximum of 30 hops:

  1     6 ms     7 ms     5 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   111 ms    54 ms    53 ms  10.64.198.161
  4    83 ms    58 ms    72 ms  xe3-2-0-4.helpa-gw1.fi.elisa.net [139.97.7.25]
  5    87 ms    45 ms    41 ms  sonera-gw.1.fi.elisa.net [139.97.7.26]
  6   152 ms    50 ms    59 ms  141.208.192.18
  7    58 ms    56 ms    56 ms  dsl-jklbng12-54fbdd-209.dhcp.inet.fi [84.251.221.209]

Trace complete.
```

Obrázek 4.15: *Záznam trasy mezi klientem a serverem v buňkové síti*

Tabulka 4.11: *Výsledky měření z buňkové sítě do Internetu*

			zpráva A		
Číslo testu	**ID metody**	**Prostor [b]**	**Počet zpráv**	**Čas [s]**	**Úspěch**
435.01	301	8	61	61	ne
435.02	303	16	311	317	ano
435.03	333	16	32	32	ne°
435.04	335	16	32	32	ano
435.05	703	16	32	98	ano
435.06	705	32	17	53	ano
435.07	733	64	x	x	ne
435.08	301, 303, 305, 333, 335	69	14	13	ne
435.09	703, 705	48	11	35	ano
435.12	303, 705	72	15	47	ne°

x – nebylo čekáno na dokončení odesílání z důvodu, že je přenos zřejmě poškozen

° *neočekávaný výsledek*

Datový přenos steganografického kanálu v mobilní síti vykazuje podobné znaky jako přenos při klasickém pevném připojení, kdy se opět, i když v menší míře, projevuje ztráta paketů. Dá se tvrdit, že mobilní datová síť se v případě zkoušených protokolů neliší od klasického připojení a z hlediska steganografie tohoto rozsahu je volba konektivity k Internetu irelevantní. Buňkové sítě, jako poskytovatelé nezávislého datového připojení, otevírají otázku, zdali je potřeba v nich provádět steganografii, protože, jde-li o nepozorované přenosy dat, je z hlediska administrátora lokální sítě téměř nemožné kontrolovat jejich datový provoz, protože podléhají jinému dozoru obvykle ze strany mobilního operátora.

4.4 Parametry skrytého kanálu

4.4.1 Přenosová kapacita

V této práci byl identifikován nekompletní výčet polí v hlavičkách síťových protokolů, které je možné steganograficky využít. Pokud je konkrétní pole využito, je možné zabrat celou jeho délku. Sečtením takových polí v jednom protokolu a mezi vzájemně se nevylučujícími protokoly pak získáme kompletní bitovou kapacitu zprávy.

Tabulka 4.12: *Maximální kapacita skrytého kanálu pro jednotlivé protokoly v navržených metodách*

Protokol	Režim	Prostor [b]	Metody
IP	maximální	37	301, 303, 305
IP	spolehlivý	16	303
ICMP	maximální	32	333, 335
ICMP	spolehlivý	32	333, 335
DNS	maximální	48	703, 705
DNS	spolehlivý	48	703, 705
HTTP	maximální	64	733
HTTP	spolehlivý*	64	733

**v měřeních byla tato metoda slabá vinou nevhodné implementace protokolu TCP a problému s navazováním spojení. Potenciál tohoto přístupu je značný, a proto je ponechán v přehledu.*

V měřeních se ukázalo, že některé metody fungují spíše teoreticky, či jen v lokálních sítích, proto bylo v přehledu přistoupeno k rozlišení hodnoty maximální a doporučené (spolehlivé), kterou by bylo možné skutečně použít pro prostředí Internetu.

V poměru velikosti všech síťových hlaviček a kapacity skrytého kanálu je prostor pro vlastní data hodnocen jako malý. Jisté snížení propustnosti také způsobuje vlastnost implementace, kdy je nutné přenést úvodní nulu samostatně, pokud ní začíná část právě zpracovávaného podřetězce z binárního řetězce celé tajné zprávy. Tuto vlastnost rozkrývá následující tabulka.

Tabulka 4.13: *Přehled efektivity metod pro přenos zprávy A*

Metoda	Zpráv A	Bloků A celkem	Bloků A nula	Podíl nulových bloků A [%]
301	61	61	2	3,39
303	311*	32	2	6,25
333	32	32	2	6,25
335	32	32	2	6,25
703	32	32	2	6,25
705	17	17	2	11,76
733	10	10	2	20,00
301, 303, 305, 333, 335	14	58	14	24,14
303, 305, 333, 335	19	59	19	32,20
303, 333, 335	15	32	2	6,25
333, 335	16	32	2	6,25
703, 705	11	22	2	9,09
301, 705	13	25	2	8,00
303, 705	15	19	2	10,53

**informace je obsažena ve 32 zprávách ze zachycených 311. 279 zpráv obsahovalo prázdný ping simulující běžné chování systému*

Tabulka 4.14: *Přehled efektivity metod pro přenos zprávy B*

Metoda	Zpráv B	Bloků B celkem	Bloků B nula	Podíl nulových bloků B [%]
301	256	256	34	13,28
303	1221*	123	10	8,13
333	123	123	10	8,13
335	123	123	10	8,13
703	123	123	10	8,13
705	67	57	10	17,54
733	31	31	2	6,45
301, 303, 305, 333, 335	57	233	65	27,90
303, 305, 333, 335	69	213	56	26,29
303, 333, 335	59	123	10	8,13
333, 335	62	123	10	8,13
703, 705	43	86	10	11,63
301, 705	46	92	2	2,17
303, 705	58	73	10	13,70

**informace je obsažena ve 123 zprávách ze zachycených 1221. 1098 zpráv obsahovalo prázdný ping simulující běžné chování systému*

Z tabulek zjevně vyplývá, že u metod, které odebírají z celkového binárního řetězce bloky stejných délek dojde ke stejnému zpracování podřetězců v případě výskytu úvodní nuly.

Hodnocení této implementace modulace tajné zprávy do hlaviček protokolů je snazší u metod, které nejsou zkombinovány s jinými. Vyplývá, že samostatné metody pro zprávy A a B mohou odeslat od 3 do 20 % zpráv navíc podle rozložení nulových znaků ve zdrojovém řetězci, průměrně jde o hodnotu 9,25 %. Procentuální výpočet však nezohledňuje kapacitu metody ani další faktory jako prodlevu, jen statisticky oznamuje, že reálná efektivita přenosu je v rozmezí 70 až 97 % z dosažitelné přenosové kapacity pro samostatné metody. Situace u kombinovaných metod je otevřenější, kdy je podíl nulových bloků k celým 2 až 32 %, průměrně pak 13 %.

Ze zjištěných hodnot nelze usuzovat další závěry, protože statistická data z přenosu dvou řetězců jsou příliš malá, rozložení přenosových kapacit metod není dostatečně reprezentativní ani výskyty znaků „0“ ovlivňující počty nulových zpráv nejsou normalizovány. V konkrétním případě platí, že pro zprávu A je nejefektnější na počet zpráv přenos metodou 301, pro zprávu B je to kombinace metod 301 a 705.

4.4.2 Rychlost

Steganografické metody používají běžný síťový provoz, který následuje rychlost přenosového média. Vypočítaná bitová rychlost skrytého kanálu je pro sledované metody uvedena v tabulce 4.16, ze soudobého hlediska jde však o velice pomalý přenos. Hlavním rychlostním omezením při přenosu je velikost použitých hlaviček a vyčkávání na odpověď protistrany. Toto vyčkávání bylo ve většině metod implementováno staticky, tedy nezávisle na skutečně obdržené odpovědi, aby se dodržovala zvyklost konkrétních implementací nástrojů používající tyto protokoly (například ICMP ping v operačním systému Windows). V některých případech bylo vyčkávání potřeba, protože se v mezičase sestavovala regulérní odpověď za použití reálné služby (DNS požadavek). Metody

využívající protokolu IP pak nelze vysílat samostatně (proto nemá smysl zmiňovat jejich prodlevu) a musí být přidruženy k některému jinému protokolu (ICMP, DNS), ze kterých vychází jejich čas vyčkávání.

Problému s prodlevami s cílem zvýšení přenosové rychlosti se lze zbavit jednoduše zkrácením intervalů (za cenu rizika odhalení), nebo s náročnější variantou implementace, kdy se otevírá naslouchání po odeslání s následnou reakcí. V základní verzi byl požadován kanál jednosměrný, ve kterém tato vlastnost není potřeba. Některé standardní implementace metod operačními systémy navíc vyčkávají i po přijetí odpovědi (ICMP ping). Kde je známo, že naslouchání zrychluje provoz, jsou metody využívající transportní protokol TCP.

Tabulka 4.15: *Přehled dosažených bitových rychlostí v internetu i místní síti pro obě zprávy*

Metoda	Prostor [b]	Čas A [s]	Zpráv A	Rychlost A [b/s]	Čas B [s]	Zpráv B	Rychlost B [b/s]
301	8	60	61	8,13	256	256	8,00
303	16	311	32	1,65	1227	123	1,60
333	16	31	32	16,52	122	123	16,13
335	16	31	32	16,52	123	123	16,00
703	16	94	32	5,45	368	123	5,35
705	32	50	17	10,88	200	67	10,72
733	64	76	10	8,42	229	32	8,94
301, 303, 305, 333, 335	69	13	14	74,31	56	57	70,23
303, 305, 333, 335	61	18	19	64,39	68	69	61,90
303, 333, 335	48	14	15	51,43	58	59	48,83
333, 335	32	15	16	34,13	61	62	32,52
703, 705	48	31	11	17,03	127	43	16,25
301, 705	40	37	13	14,05	136	46	13,53
303, 705	48	43	15	16,74	172	58	16,19

Tabulka 4.16: *Přehled dosažených bitových rychlostí při specificky nastavených časovačích*

Metoda	Nosný protokol	Průměrná rychlost [b/s]
301, 303, 305, 333, 335	ICMP	72,3
303, 305, 333, 335	ICMP	63,1
303, 333, 335	ICMP	50,1
333, 335	ICMP	33,3
703, 705	DNS	16,6
303, 705	DNS	16,5
333	ICMP	16,3
335	ICMP	16,3
301, 705	DNS	13,8
705	DNS	10,8
733	HTTP	8,7
301	IP	8,1
703	DNS	5,4
303	IP	1,6

4.4.3 Spolehlivost

Jedním ze základních předpokladů při vytváření kanálu je jistota, že obdržíme data ve stejné podobě, v jaké byla odeslána. Prvním z požadavků je rozpoznání porušení konzistence, čehož bylo dosaženo připojováním řetězce s kontrolním hashem. V průběhu testování se ukázalo, že navržený způsob spolehlivě rozpozná, pokud přijatý řetězec není v pořádku.

Implementované řešení v dokončené verzi postrádá další prvky ochrany zvyšující spolehlivost. Je spoléháno na v praxi používaný princip největšího úsilí při doručení, kdy většina provozu prochází sítí tak, jak byla odeslána. Nenastane-li zahlcení některého z nácestných uzlů nebo výpadek na trase, není potřeba dalších mechanismů, protože síť sama o sobě preferuje doručení celého toku dat v pořadí a symetrickou trasou. Tento předpoklad v praxi nefungoval, respektive byl účinný pouze v lokálních metalických sítích a na rozhraní zpětné smyčky. Bezdrátový přenos s horším signálem vyžaduje, jak ukázalo měření, nějaký druh zajištění spolehlivosti přenosu nebo redundance ve zprávě samotné.

Implementace spolehlivosti přenosu není triviální, protože je umožněno kombinování steganografické zprávy přes více protokolů, kdy by bylo potřeba doplnit mechanismus, který si ukládá, která část z řetěze byla umístěná v konkrétní odeslané zprávě, a zopakovat toto vysílání, je-li o to požádáno. V praxi se několikrát vyskytl případ ztráty datagramu, kdy klient začal vysílat ještě před připravením serveru k poslechu, tuto chybu by bylo možné odstranit doplněním mechanismu sestavení spojení, který byl navržen v přechozích kapitolách. Zahození paketů na trase se v testovaných případech vyskytovalo, a lze tak tvrdit, že tento problém není zanedbatelný. Rozhodující vliv na spolehlivost přenosu má v dané implementaci kvalita dostupného síťového spojení a vytížení síťových prvků.

S tématem spolehlivosti úzce související se steganografií se stalo přepisování některých polí směrovači na okrajích sítí, respektive při vstupu do nich. Typickým představitelem je pole DiffServ hlavičky protokolu IP, které se standardně používá k zajištění kvality služby (QoS) a které může sloužit k prioritizaci některého datového provozu před jiným, čehož by mohlo být zneužito. V praxi se pak přistupuje k dohledu nad touto hodnotou a nedůvěře v nastavení priority pocházející z příchozího provozu jiné sítě, případně přímo od klientských stanic. Během měření bylo ověřeno, že ukrývat steganografická data do těchto polí má význam pouze v některých lokálních sítích a při průchodem Internetu je hodnota vždy přepsána a data ztracena. U složených metod používající toto pole pak dojde k poškození celé přijaté zprávy.

Při reálném používání steganografického programu ve vyhotovené verzi je nutné uvažovat o nejméně jednom redundantním opakování vysílání zprávy pro zaručení doručení zprávy. Zvýšit šanci pro doručení oproti předchozímu vysílání může také použití jiné metody nebo jejich odlišná kombinace.

4.4.4 Vliv na síťový provoz

Návrh steganografického kanálu nepočítal s vlivem na okolní provoz, což se v praxi potvrdilo, protože nebylo využíváno metody modifikace okolního provozu, ale oba uzly, jak server, tak klient jsou původci steganografické komunikace. Stejně jako v ostatních síťových aplikacích se používá k oddělení toků dat kombinace IP adresa – port, která zajišťuje, že provoz není spojen s jiným.

Prakticky se projevilo jako nevhodné řešení navazující komunikaci striktně z určitého portu a IP adresy, neboť do trasy může vstoupit překlad adresy (NAT) či portu (PAT), který změní síťové

hodnoty (v případě PAT například zdrojový port). Ačkoliv tak úvodní datagram dorazí na aktivní server, není na něj reagováno. Toto řešení nelze dále rozvíjet a je třeba doplnit další metodu rozpoznání steganografie zmíněnou v části Sestavení spojení. Tento nedostatek byl shledán jako největším ve vztahu k okolnímu provozu a síťovým principům. V zásahům do cílových portů nedocházelo, neboť bylo používáno rozsahů pro dynamické porty a také standardní porty jako 80 či 53.

Bez ovlivnění výsledků se projevilo tunelování provozu při měření ve virtuální privátní síti (VPN). Situace je jednak daná principem fungování této technologie, která nezasahuje do stávajících hlaviček, a také důsledkem skutečnosti, že přenášené zprávy jsou krátké bez plného využití polí pro přenášení data. Připojení hlaviček nutných pro tunelování nezpůsobí fragmentaci, protože není překročena maximální přenosová jednotka (MTU), tedy velikostní omezení v bajtech pro celý samostatný datagram.

V prostředí akademické sítě VŠB-TUO se projevila komplikace, kdy správci z bezpečnostních důvodů blokují jiné DNS servery než své vlastní, takže datový provoz směřující na podvržený DNS server zachycující steganografii byl zablokován. Toto provozní omezení prakticky blokuje skryté kanály využívající DNS na standardním UDP portu, protože po změně portu byly stejné datagramy doručeny a zpracovány.

4.4.5 Hodnocení výsledků

Výsledky v uvedených měřeních zásadně nepřekvapují a odpovídají nastaveným očekáváním. Jak bylo předpokládáno, v místní síti je možné odesílat téměř jakýkoliv provoz zahrnující steganografický, protože standardně nasazené síťové uzly jsou benevolentní v doručení zpráv, i pokud nejsou všechny údaje v hlavičkách správně vyplněny (MAC adresy), či je zapisováno do polí určování priority zpracování.

Hodnocení výsledků v síti Internet je výrazně ovlivněno nedokonalou implementací, která postrádá zajištění spolehlivosti a ovlivnění výsledků ztrátou paketů. Jako nedostatečné se ukázalo programové zpracování metody používající protokol HTTP, respektive jeho spojení s vlastní implementací protokolu TCP, který i přes veškerou snahu nereagoval podle standardů a nebyl tedy prakticky použitelný.

Obecně lze však říci, že nejvíce prostoru, při správném vyladěním časovačů, poskytují protokoly aplikačních vrstev, které lze doporučit. DNS a HTTP společně s protokolem ICMP vytvářejí vhodný nosič pro steganografii přes síť Internet. Běžným způsobem konfigurovaná síťová prostředí umožňují přenos skrytého kanálu. V chráněných prostředích je potřeba si ověřit, zdali je provoz, který zamýšlíme využít, možné směrovat k uzlu zpracovávající steganografii, a jaké další ochranné mechanismy se síti vyskytují.

Závěr

Tato práce potvrdila existující předpoklad, že vytvoření steganografie v síťovém prostředí TCP/IP je možné na takových vrstvách referenčního modelu, který umožní úspěšný průchod sítí Internet. Ukázalo se, že prostor pro hledání nových metod v nižších vrstvách je již vyčerpán. Kde v současnosti lze najít nový potenciál jsou hlavičky aplikačních protokolů, které se stále vyvíjejí a procházejí standardizačním procesem, čímž poskytují krytí steganografii a zároveň poměrně vysokou kapacitu v porovnání s vrstvami nižšími. Vyplynulo, že nejvhodnějšími místy pro ukrývání zpráv jsou ta, která jsou inicializována náhodnou hodnotou, kdy je možné tuto hodnotu účelově nahradit. Riziko odhalení zvyšuje využívání částí hlaviček, které nemají vliv na doručení datagramu, avšak v praxi se používají výjimečně nebo jsou již považované za zastaralé.

Práce se zabývala rodinou protokolů TCP/IP, kam patří i protokol IP verze 4, jehož struktura hlaviček je pevně určená, situace v nahrazujícím protokolu IP verze 6 je odlišná. Modernější verze poskytuje možnost připojovat hlavičky podle potřeby, z časových důvodů nebyla steganografie v tomto protokolu implementována. Rozšíření stávajícího kódu praktické části je na tuto možnost připraveno. Steganografie byla úspěšně umístěna do protokolu ICMP, avšak jako nevýhoda se v praxi projevilo, že tento protokol je z bezpečnostních důvodů v některých prostředích blokován. Spojením metod protokolů IP a ICMP vznikl kanál, který poskytnul nejvyšší přenosovou rychlost z vytvořených řešení. Na transportní vrstvě bylo zadáním omezeno používání protokolu UDP jako nosného, proto zůstalo používání protokolu TCP, který poskytuje prostor pro steganografii, avšak příliš zjevným způsobem, který je snadný na odhalení. Skrytý kanál se podařilo úspěšně umístit do protokolů aplikačních vrstev DNS a HTTP, kde byla nalezena dostatečná přenosová kapacita a zároveň dobrá průchodnost sítí Internet.

Přínos práce je ve vyhotovení nástroje pro průzkum steganografických metod a jejich testování v různých TCP/IP sítích. Přidaná hodnota je v možnosti kombinovat více vrstev referenčního modelu při vytváření netriviálního skrytého kanálu. Proti jednoduchým nástrojům vkládající data jen do přesně stanovených míst v záhlaví poskytuje výhodu práce se záhlavím protokolů jako s objekty. Ve stávající podobě umožňuje jednoduché přidávání dalších metod a jejich testování kombinováním s již existujícími. Návrh programu byl proveden mohutně s množstvím obslužných metod s ideou oddělení jako knihovny. V této implementaci byl klient a server koncovým uzlem komunikace, avšak při plánování architektury programu bylo uvažováno i o průchozí roli.

Ve steganografii platí přímá úměra, že se snižující se potřebnou kapacitou přenosu a požadavkem na rychlost se možnosti jejího odhalení dramaticky snižují. Zásadní je také vliv okolního prostředí, ve kterém při dostatečném ostatním síťovém provozu vlastní steganografická komunikace dokáže splynout s okolím. Nejsnadnější implementací je přímá komunikace dvou síťových uzlů v roli serveru a klienta, zde však musí počítat návrhář se skutečností, že je obtížné ukrýt síťovou adresu zdroje a cíle proto, že je potřebná pro doručení. Při jakémkoliv komplexnějším návrhu například využívajícím proxy server je pak potřeba řešit nejen vlastní směrování provozu těmito body, ale také značně zvýšenou režii při sestavování zpráv a převodu do uživatelských dat.

Při návrhu nového kanálu se vyplácí používat řešení, která buď věrně napodobují jiné služby komunikující po téže síti, nebo je přímo využívají jako nosiče, v práci byla aplikována metoda HTTP požadavků na podvržený server některé ze sociálních sítí, které využívají dlouhé řetězce jako

identifikátory multimediálních dat i samotných stránek, které byly nahrazeny vlastními daty (při vyloučení funkcionality). V celkovém pohledu však lze říci, že steganografie v síťovém prostředí neposkytuje mnoho prostoru pro přenos dat.

Nabízí se otázka, proč tuto technicky komplikovanou činnost provádět. Tato práce identifikovala další případy užití. Jednou ze základních teorií byla potřeba dopravit nějakou citlivou informaci (například privátní klíč certifikátu) ze střeženého prostředí. V závislosti na stupni ochrany však bude obtížné inicializovat síťovou komunikaci do či přes takové uzly, které nevzbudí podezření dozorce. Pokud neexistuje tato omezující podmínka, pak je otázkou, zdali je třeba využívat steganografii k přenosu informace a zdali by nešlo data odeslat jakoukoliv jinou konvenční metodou. Tato úvaha se zdá být rozuzlením otázky širšího využívání techniky steganografie k přenosu informací v prostředí počítačových sítí ve smyslu utajení komunikace.

Druhou, novější, teorií, která byla ověřena, je možnost používání steganografie k ovládání uzlů mající přístup k síti zasíláním instrukcí v situacích, kdy by zablokování standardní komunikace způsobilo jejich izolaci. Prakticky toto pojetí zahrnuje negativní scénář ovládání botnetu, nebo pozitivní scénář komunikace nodů v rámci honeypotu (prostředí zachytávání softwarových hrozeb). V obou případech může docházet ke sledování okolního provozu a polymorfním reakcím ochránce nebo útočníka. Utajený, respektive nestandardní, způsob komunikace může zajistit, že účastníci této komunikace mohou být aktivnější s nižším rizikem odhalení.

Třetí ověřenou teorií je možnost využití steganografických metod jako technických prostředků k přenosu dat překonávající síťová omezení. V tomto pojetí je potřeba komunikaci skrývat sekundární, protože primárním cílem je zajistit vlastní spojení, které je přerušeno například obsahovým filtrem (v extrémním případě cenzurou), firewallem, omezením přístupu k přenosovému médiu apod. Toto pojetí se nazývá tunelování, nicméně tytéž metody používané v oboru stenografie jsou v něm také hojně zastoupeny. Tato práce popsala některé z jejich technik a určila u nich kapacitu přenosového kanálu.

Shrnutí: Využití síťové steganografie má své specifické podmínky. Ve starším pojetí jde o přenos utajené zprávy, nové uplatnění je pak realizace komunikace zejména v prostředích, které jsou nějakým způsobem omezen, kdy je cílem překonání této obstrukce. Posledním scénářem je vytvoření obtížně přerušitelného či detekovatelného spojení. Tato práce tak objasnila možné případy užití a prakticky ověřila, že je možné jich technicky dosáhnout a určila jejich specifické parametry.

Použitá literatura a zdroje

[1] Bridgeguys. Bridgeguys.com [online]. online: online, 2018 [cit. 2018-04-03]. Dostupné z: http://www.bridgeguys.com/sec/glossary/b/index.html

[2] Bridž. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2017-04-03]. Dostupné z: https://cs.wikipedia.org/wiki/Brid%C5%BE

[3] Steganografie [online]. Brno, 2017 [cit. 2018-04-03]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7030. Opora. Mendel University.

[4] ŽILKA, Bc. Roman. Steganografie a stegoanalýza [online]. Brno, 2008 [cit. 2018-04-03]. Dostupné z: https://is.muni.cz/th/73058/fi_m/Steganografie_a_stegoanalyza.pdf. Diplomová práce. Masarykova univerzita.

[5] Hierarchie Data → Informace → Znalost. Wikisofia [online]. online: online, 2017 [cit. 2018-04-03]. Dostupné z: http://wikisofia.cz/wiki/Hierarchie_Data_%E2%86%92_Informace_%E2%86%92_Znalost

[6] J. SIMMONS, Gustavus. The prisoner's problem and the subliminal channel [online]. online, 1998 [cit. 2018-04-03]. Dostupné z: http://www.cs.nccu.edu.tw/~raylin/UndergraduateCourse/ComtenporaryCryptography/Spring2009/ThePrisonerProblem.pdf. článek. Sandia National Laboratories Albuquerque.

[7] STEGANONET – Evolution *of Steganography* (video) [cit. 2018-04-03]. Dostupné z: https://www.youtube.com/watch?v=osNWSGsFOvA

[8] Two Generals' Problem. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-03]. Dostupné z: https://en.wikipedia.org/wiki/Two_Generals%27_Problem

[9] Linguistic Steganography: Information Hiding in Text [online]. Edinburgh, 2012 [cit. 2018-04-03]. Dostupné z: https://www.cl.cam.ac.uk/~sc609/talks/ed12stego.pdf. Prezentace. University of Cambridge Computer Laboratory.

[10] Velvalee Dickinson. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-03]. Dostupné z: https://en.wikipedia.org/wiki/Velvalee_Dickinson

[11] Mgr. Tomáš Foltýnek, Ph.D., Ing. Jan Přichystal, Ph.D. Komprimace a šifrování [online]. Brno, 2010 [cit. 2018-04-03]. Dostupné z: https://akela.mendelu.cz/~foltynek/KAS/elearning/KAS_PDF.pdf. Podpora. Mendelova univerzita v Brně.

[12] Podprahový signál. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-03]. Dostupné z: https://cs.wikipedia.org/wiki/Podprahov%C3%BD_sign%C3%A1l

[13] EURion constellation. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-03]. Dostupné z: https://en.wikipedia.org/wiki/EURion_constellation

[14] Detekce barev a bankovek pro nevidomé uživatele v prostředí Android [online]. Praha, 2012 [cit. 2018-04-03]. Dostupné z: https://dspace.cvut.cz/bitstream/handle/10467/61127/F3-DP-2015-Pechan-Jan-pechaja6_dp.pdf. Diplomová práce. České vysoké učení technické v Praze.

[15] InfoBiology by printed arrays of microorganism colonies for timed and on-demand release of messages. PNAS [online]. 2011, 2011(October 4), 108 (40) [cit. 2018-04-03]. ISSN 16510-16514. Dostupné z: http://www.pnas.org/content/108/40/16510

[16] James Collins a Sos Agaian. TRENDS TOWARD REAL-TIME NETWORK DATA STEGANOGRAPHY [online]. San Antonio, USA, 2010 [cit. 2018-04-03]. Dostupné z: https://arxiv.org/ftp/arxiv/papers/1604/1604.02778.pdf. Article. University of Texas at San Antonio.

[17] Information Technologies for IPR Protection: Steganography [online]. Taiwan, 2010 [cit. 2018-04-03]. Dostupné z: http://www.cmlab.csie.ntu.edu.tw/~ipr/ipr2006/data/lecture/Lecture11%20-%20Steganography.pdf. Prezentace. Csie.ntu.edu.tw.

[18] Steganografická komunikace [online]. Zlín, 2006 [cit. 2018-04-03]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/2351/zigulec_2006_dp.pdf?sequence=1. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

[19] COUTURE, E. Covert Channels [online]. SANS Institute. 2010 [cit. 2012-02-01]. Dostupné z: http://www.sans.org/reading_room/whitepapers/ detection/covert-channels_33413

[20] Implementace skrytých kanálů v IPv6 [online]. Brno, 2012 [cit. 2018-04-03]. Dostupné z: https://is.muni.cz/th/359251/fi_b/bc.pdf. Bakalářská práce. Masarykova univerzita.

[21] NOVOTNÝ, Marián. Skryté kanály v sieťových protokoloch. ESET, spol. s r.o. [online]. [cit. 2018-04-03]. Dostupné z: https://www.youtube.com/watch?v=p5oQlfkiwcE

[22] Covert Channels in Network protocols. In: NOVOTNÝ, Marián. : Bez(a)Dis [online]. Košice, 2011 [cit. 2018-04-03]. Dostupné z: https://bezadis.ics.upjs.sk/pub/resources/marian-novotny/slajdy.pdf

[23] BRINKMANN, Martin. Blizzard watermarking WoW screenshots. GHack.net [online]. 2012 [cit. 2018-04-03]. Dostupné z: https://www.ghacks.net/2012/09/12/blizzard-watermarking-wow-screenshots/

[24] STRÁNSKÝ, Petr. Historie Wi-Fi: od FHSS k bezdrátu [online]. 2009 [cit. 2018-04-03]. Dostupné z: https://www.svethardware.cz/historie-wi-fi-od-fhss-k-bezdratu/27860

[25] PETERKA, Jiří. Síťový model TCP/IP. Vyšlo v týdeníku Computerworld č. 31/92 v roce 1992 [online]. 2015, 1992, díl/část č.: 42 [cit. 2018-04-04]. Dostupné z: http://www.earchiv.cz/a92/a231c110.php3

[26] Téma 10 – Síťové IP protokoly a API [online]. Praha, 2013 [cit. 2018-04-04]. Dostupné z: http://labe.felk.cvut.cz/vyuka/A4B33OSS/Tema-10-Site-Protokoly.ppt. Prezentace. ČVUT.

[27] Lukas C#. Sítě – Internet protokol – hlavička: 5. díl [online]. 2015, , 1 [cit. 2018-04-04]. Dostupné z: https://www.itnetwork.cz/site/internet-protokol-hlavicka

[28] Evil bit: Internet Engineering Task Force RFC standards. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-04]. Dostupné z: https://en.wikipedia.org/wiki/Evil_bit

[29] PETERKA, Jiří. Počítačové sítě I, lekce 3: Vrstvy a vrstvové modely: **slide 23**. Slideshare.net [online]. 30.9.2017, 32 [cit. 2018-04-04]. Dostupné z: https://www.slideshare.net/jiri.peterka/l3-39692790

[30] PETERKA, Jiří. Počítačové sítě I, lekce 3: Vrstvy a vrstvové modely: **slide 25**. Slideshare.net [online]. 30.9.2017, 32 [cit. 2018-04-04]. Dostupné z: https://www.slideshare.net/jiri.peterka/l3-39692790

[31] OCHODKOVÁ, Ph.D., RNDr. Eliška. Kryptografie a počítačová bezpečnost [online]. Ostrava, 2007 [cit. 2018-04-04]. Dostupné z: wiki.cs.vsb.cz/images/a/a9/Kb07.pdf. Přednáška. Vysoká škola Báňská – Technická univerzita Ostrava.

[32] SILBERSACK, Michael James. Improving TCP/IP security through randomization without sacrificing interoperability: The FreeBSD Project [online]. , 17 [cit. 2018-04-06]. Dostupné z: http://www.silby.com/eurobsdcon05/eurobsdcon_silbersack.pdf

[33] Knihovna Winpcap: a její základní použití. Root.cz [online]. 18. 10. 2006, , 1 [cit. 2018-04-04]. Dostupné z: https://www.root.cz/clanky/knihovna-winpcap-a-jeji-zakladni-pouziti/

[34] Samodetekující kód. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-04]. Dostupné z: https://cs.wikipedia.org/wiki/Samodetekuj%C3%ADc%C3%AD_k%C3%B3d

[35] Cisco Networking Academy [online]. online: Cisco Press, 2016 [cit. 2018-04-04]. Dostupné z: https://www.netacad.com/

[36] TCP Priority Data Transfer: "Urgent" Function: Prioritizing Data For Transfer. The TCP/IP Guide [online]. [cit. 2018-04-04]. Dostupné z: http://www.tcpipguide.com/free/t_TCPPriorityDataTransferUrgentFunction-2.htm

[37] RFC1035: DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION. Dostupné z: https://tools.ietf.org/html/rfc1035#section-4.1.1: IETF, 1987.

Seznam příloh

Příloha na CD/DVD.

Zdrojové kódy také v repozitáři GitHub https://github.com/microkost/Steganography-for-IP-networks

Adresářová struktura přiloženého CD/DVD:

```
+
|
+---packages
|
+---records
|   +---direct
|   +---internet-citywifi
|   +---internet-vsb
|   +---localhost
|   +---mobile
|   \---wifi
|
+---releases
|
+---SteganoNet.Lib
|   +---graphic
|   \---Properties
|
+---SteganoNet.Tests|   |
|   \---Properties
|
+---SteganoNet.UI.Console
|   \---Properties
|
+---SteganoNet.UI.WinForms
|   \---Properties
|
\---testing
```